Panduan Referensi

AWS Manajemen Akun

AWS Manajemen Akun: Panduan Referensi

Table of Contents

Selamat datang 1
Apakah saya membutuhkan beberapaAkun AWS? 2
Mengelola beberapaAkun AWS 3
Memulai: Apakah Anda AWS pengguna pertama kali? 3
Prasyarat 3
Langkah 1: Buat Akun AWS 5
Langkah 2: Aktifkan MFA untuk pengguna root Anda 6
Langkah 3: Buat pengguna administrator 7
Topik terkait 7
Menggunakan pengguna root 7
Kelola akun Anda 9
Buat akun Anda 9
Lihat pengenal akun Anda 12
Temukan Akun AWS ID Anda 13
Temukan ID pengguna kanonik untuk Anda Akun AWS 15
Perbarui pengaturan akun Anda 18
Memahami mode operasi API 20
Memberikan izin untuk memperbarui atribut akun 21
Memperbarui informasi kontak akun 23
Kontak akun alternatif 23
Kontak akun utama 33
Perbarui pertanyaan tantangan keamanan Anda 39
Tentukan Wilayah AWS akun mana yang dapat digunakan 41
Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah 42
Mengaktifkan atau menonaktifkan Region untuk akun mandiri 44
Mengaktifkan atau menonaktifkan Wilayah di organisasi Anda 47
Buat atau perbarui alias akun Anda 49
Tagihan AndaAkun AWS 49
Mengelola akun di India 50
Tentukan perusahaan mana akun Anda 50
Buat sebuahAkun AWSdengan AISPL 51
Kelola akun AISPL Anda 53
Tutup akun Anda 53
Apa yang perlu Anda ketahui sebelum menutup akun Anda 53

Cara menutup akun Anda 55
Apa yang diharapkan setelah Anda menutup akun Anda 58
Manajemen Akun & AWS Organizations 60
Akses tepercaya 61
Akun admin yang didelegasikan 62
Contoh SCP 64
Keamanan 67
Perlindungan data 68
AWS PrivateLink 69
Membuat Titik Akhir 69
Kebijakan Amazon VPC Endpoint 70
Kebijakan Titik Akhir 70
Manajemen Identitas dan Akses 71
Audiens 72
Mengautentikasi dengan identitas 72
Mengelola akses menggunakan kebijakan 76
AWSManajemen Akun dan IAM 79
Contoh kebijakan berbasis identitas 87
Menggunakan kebijakan berbasis identitas 91
Memecahkan masalah 93
Kebijakan yang dikelola AWS 95
AWSAccountManagementReadOnlyAccess 96
AWSAccountManagementFullAccess 97
Pembaruan kebijakan 98
Validasi kepatuhan 98
Ketahanan 99
Keamanan infrastruktur 100
Memantau 101
Catatan CloudTrail 101
Informasi Manajemen Akun di CloudTrail 102
Memahami entri log Manajemen Akun 103
Memantau acara Manajemen Akun dengan EventBridge 106
Acara Manajemen Akun 106
Referensi API 109
Tindakan 111
DeleteAlternateContact 112

DisableRegion 117
EnableRegion 121
GetAlternateContact 125
GetContactInformation 130
GetRegionOptStatus 134
ListRegions 138
PutAlternateContact 143
PutContactInformation 149
Tindakan terkait 152
CreateAccount 152
CreateGovCloudAkun 152
DescribeAccount 152
Tipe Data 152
AlternateContact 154
ContactInformation 156
Region 160
ValidationExceptionField 161
Parameter Umum 161
Kesalahan Umum 164
Membuat permintaan Kueri HTTP 165
Titik akhir 166
HTTPS diperlukan 167
PenandatangananAWSPermintaan API Manajemen Akun 167
Quotas 168
Memecahkan masalah Anda Akun AWS 170
Masalah pembuatan akun 170
Saya tidak menerima panggilan dari AWS untuk memverifikasi akun baru saya 170
Saya mendapatkan kesalahan tentang “jumlah maksimum upaya yang gagal” ketika saya mencoba memverifikasi Akun AWS melalui telepon 171
Sudah lebih dari 24 jam dan akun saya tidak diaktifkan 172
Masalah penutupan akun 173
Saya tidak tahu cara menghapus atau membatalkan akun saya 173
Saya tidak melihat tombol Tutup akun di halaman Akun 173
Saya menutup akun saya tetapi masih belum menerima konfirmasi email 173
Saya menerima kesalahan ConstraintViolationException "" saat mencoba menutup akun saya 174

Saya menerima kesalahan “CLOSE_ACCOUNT_QUOTA_EXCEEDED” saat mencoba menutup akun anggota 174
Apakah saya perlu menghapus AWS organisasi saya sebelum menutup akun manajemen? 174
Masalah lainnya 175
Saya perlu mengubah kartu kredit untuk sayaAkun AWS 175
Saya ingin melaporkan penipuanAkun AWSaktivitas 175
Saya ingin menutupAkun AWS 175
Riwayat dokumen 176
AWSGlosarium 178
..... clxxix

Selamat datang di Panduan Referensi Manajemen AWS Akun

Akun AWSadalah bagian mendasar dari mengakses AWS layanan.

An Akun AWS melayani dua fungsi dasar:

- Container — An Akun AWS adalah wadah dasar untuk semua AWS sumber daya yang Anda buat sebagai AWS pelanggan. Misalnya, bucket Amazon Simple Storage Service (Amazon S3), database Amazon Relational Database Service (Amazon RDS), dan instans Amazon Elastic Compute Cloud (Amazon EC2) adalah semua sumber daya. Setiap sumber daya diidentifikasi secara unik oleh Amazon Resource Name (ARN) yang menyertakan ID akun akun yang berisi, atau memiliki, sumber daya.
- Batas keamanan — An juga Akun AWS merupakan batas keamanan dasar untuk sumber daya Anda. AWS Sumber daya yang Anda buat di akun tersedia bagi pengguna yang memiliki kredensi untuk akun Anda.

  Di antara sumber daya utama yang dapat Anda buat di akun Anda adalah identitas, seperti pengguna dan peran. Identitas memiliki kredensi yang dapat digunakan seseorang untuk masuk (mengautentikasi). AWS Identitas juga memiliki kebijakan izin yang menentukan apa yang dapat dilakukan pengguna (otorisasi) dengan sumber daya di akun.

  Sebagai praktik keamanan terbaik, mintalah pengguna Anda untuk menggunakan kredensil sementara saat mengakses. AWS Untuk memberikan kredensi sementara, Anda dapat menggunakan federasi dan penyedia identitas, seperti AWS IAM Identity Center(IAM Identity Center). Jika perusahaan Anda sudah menggunakan penyedia identitas, gunakan dengan federasi untuk menyederhanakan cara Anda menyediakan akses ke sumber daya di AndaAkun AWS.

  Untuk informasi tentang praktik terbaik keamanan, lihat Praktik terbaik keamanan di IAM di Panduan Pengguna IAM.

Topik

- Apakah saya membutuhkan beberapaAkun AWS?
- Memulai: Apakah Anda AWS pengguna pertama kali?
- Menggunakan Pengguna root akun AWS

Apakah saya membutuhkan beberapaAkun AWS?

Akun AWSberfungsi sebagai batas keamanan mendasar diAWS. Mereka berfungsi sebagai wadah sumber daya yang menyediakan tingkat isolasi yang berguna. Kemampuan untuk mengisolasi sumber daya dan pengguna adalah persyaratan utama untuk membangun lingkungan yang aman dan tertata dengan baik.

Memisahkan sumber daya Anda menjadi terpisahAkun AWSmembantu Anda mendukung prinsip-prinsip berikut di lingkungan cloud Anda:

- Kontrol keamanan— Aplikasi yang berbeda dapat memiliki profil keamanan yang berbeda, membutuhkan kebijakan dan mekanisme kontrol yang berbeda di sekitar mereka. Misalnya, jauh lebih mudah untuk berbicara dengan auditor dan dapat menunjuk ke satuAkun AWSyang meng-host semua elemen beban kerja Anda yang tundukStandar Keamanan Industri Kartu Pembayaran (Payment Card Industry).
- Isolasi— SebuahAkun AWSadalah unit perlindungan keamanan. Potensi risiko dan ancaman keamanan harus terkandung dalamAkun AWStanpa mempengaruhi orang lain. Mungkin ada kebutuhan keamanan yang berbeda karena tim yang berbeda atau profil keamanan yang berbeda.
- Banyak tim— Tim yang berbeda memiliki tanggung jawab dan kebutuhan sumber daya yang berbeda. Anda dapat mencegah tim mengganggu satu sama lain dengan memindahkan mereka untuk memisahkanAkun AWS.
- Isolasi data— Selain mengisolasi tim, penting untuk mengisolasi penyimpanan data ke akun. Ini dapat membantu membatasi jumlah orang yang dapat mengakses dan mengelola penyimpanan data tersebut. Ini membantu mengandung paparan data yang sangat pribadi dan karena itu dapat membantu sesuai denganPeraturan Perlindungan Data Umum Uni Eropa (GDPR).
- Proses bisnis— Unit bisnis yang berbeda atau produk mungkin memiliki tujuan dan proses yang sama sekali berbeda. Dengan beberapaAkun AWS, Anda dapat mendukung kebutuhan khusus unit bisnis.
- Penagihan— Akun adalah satu-satunya cara yang benar untuk memisahkan item pada tingkat penagihan. Beberapa akun membantu memisahkan item pada tingkat penagihan di seluruh unit bisnis, tim fungsional, atau pengguna individual. Anda masih bisa mendapatkan semua tagihan Anda dikonsolidasikan ke pembayar tunggal (menggunakanAWS Organizationsdan penagihan konsolidasi) sementara memiliki item baris dipisahkan olehAkun AWS.
- Alokasi kuota—AWSkuota layanan diberlakukan secara terpisah untuk masing-masingAkun AWS. Memisahkan beban kerja menjadi berbedaAkun AWSmencegah mereka mengkonsumsi kuota satu sama lain.

Semua rekomendasi dan prosedur yang dijelaskan dalam dokumen ini sesuai denganAWSKerangka Well-Architected. Kerangka kerja ini dimaksudkan untuk membantu Anda merancang infrastruktur cloud yang fleksibel, tangguh, dan terukur. Bahkan ketika Anda mulai kecil, kami sarankan Anda melanjutkan sesuai dengan panduan ini dalam kerangka kerja. Melakukannya dapat membantu Anda meningkatkan lingkungan Anda dengan aman dan tanpa memengaruhi operasi Anda yang sedang berlangsung saat Anda tumbuh.

Mengelola beberapaAkun AWS

Sebelum Anda mulai menambahkan beberapa akun, Anda akan ingin mengembangkan rencana untuk mengelolanya. Untuk itu, kami sarankan Anda menggunakanAWS Organizations, yang gratisAWSlayanan untuk mengelola semuaAkun AWSdi organisasi Anda.

AWSjuga menawarkanAWS Control Tower, yang menambahkan lapisanAWSdikelola otomatisasi ke Organizations dan secara otomatis mengintegrasikannya dengan yang lainAWSlayanan sepertiAWS CloudTrail,AWS Config, Amazon CloudWatch,AWS Service Catalog, dan lain-lain. Layanan ini dapat dikenakan biaya tambahan. Untuk informasi lebih lanjut, lihat Harga AWS Control Tower.

Memulai: Apakah Anda AWS pengguna pertama kali?

Jika Anda adalah pengguna pertama kaliAWS, langkah pertama Anda adalah mendaftar untuk. Akun AWS Saat Anda mendaftar, AWS buat Akun AWS dengan detail yang Anda berikan dan berikan akun kepada Anda. Setelah Anda membuatAkun AWS, masuk sebagai pengguna root, aktifkan otentikasi multi-faktor (MFA) untuk pengguna root, dan tetapkan akses administratif ke pengguna.

Langkah-langkah

- Prasyarat
- Langkah 1: Buat Akun AWS
- Langkah 2: Aktifkan MFA untuk pengguna root Anda
- Langkah 3: Buat pengguna administrator
- Topik terkait

Prasyarat

Untuk mendaftarAkun AWS, Anda memerlukan informasi berikut:

- Nama akun — Nama akun muncul di beberapa tempat, seperti pada faktur Anda, dan di konsol seperti dasbor Billing and Cost Management dan konsol. AWS Organizations

  Kami menyarankan Anda menggunakan cara standar untuk memberi nama akun Anda sehingga Anda dapat memberikan nama akun Anda yang mudah dikenali. Untuk akun perusahaan, pertimbangkan untuk menggunakan standar penamaan seperti organisasi - tujuan - lingkungan (misalnya, AnyCompany- audit - prod). Untuk akun pribadi, pertimbangkan untuk menggunakan standar penamaan seperti nama depan - nama belakang - tujuan (misalnya, paulo-santos-testaccount).

  Untuk informasi tentang mengubah nama akun, lihat Bagaimana cara mengubah nama di akun sayaAkun AWS? .

- Alamat - Jika alamat kontak Anda berada di India, perjanjian pengguna untuk akun Anda adalah dengan Amazon Internet Services Private Limited (AISPL), AWS penjual lokal di India. Anda harus memberikan CVV Anda sebagai bagian dari proses verifikasi. Anda mungkin juga harus memasukkan kata sandi satu kali, tergantung pada bank Anda. AISPL membebankan metode pembayaran Anda 2 INR sebagai bagian dari proses verifikasi. AISPL mengembalikan 2 INR tersebut setelah verifikasi selesai.
- Alamat email — Alamat email digunakan sebagai nama masuk untuk pengguna root dan diperlukan untuk pemulihan akun. Anda harus dapat menerima pesan email yang dikirim ke alamat ini. Sebelum Anda dapat melakukan tugas-tugas tertentu, Anda harus memverifikasi bahwa Anda memiliki akses ke email yang dikirim ke alamat ini.

  > **Important**
  >
  > Jika akun ini untuk bisnis, gunakan daftar distribusi perusahaan yang aman (misalnya,`it.admins@example.com`) sehingga perusahaan Anda dapat mempertahankan akses ke Akun AWS bahkan ketika seorang karyawan mengubah posisi atau meninggalkan perusahaan. Karena alamat email dapat digunakan untuk mengatur ulang kredensi pengguna root akun, lindungi akses ke daftar distribusi atau alamat ini.

- Nomor telepon — Nomor ini dapat digunakan untuk mengonfirmasi kepemilikan akun Anda. Anda harus dapat menerima panggilan di nomor telepon ini.

> **Important**
>
> Jika akun ini untuk bisnis, gunakan nomor telepon perusahaan sehingga perusahaan Anda dapat mempertahankan akses ke Akun AWS bahkan ketika seorang karyawan mengubah posisi atau meninggalkan perusahaan.

Langkah 1: Buat Akun AWS

1. Di browser Anda, buka halaman AWS beranda.
2. Pilih Buat sebuah Akun AWS.

   > **Note**
   >
   > Jika Anda masuk AWS baru-baru ini, pilih Masuk. Jika opsi Buat baru Akun AWS tidak terlihat, pertama-tama pilih Masuk ke akun lain, lalu pilih Buat yang baru Akun AWS.

3. Masukkan informasi akun Anda, lalu pilih Verifikasi alamat email. Ini akan mengirimkan kode verifikasi ke alamat email yang Anda tentukan.
4. Masukkan kode verifikasi Anda, lalu pilih Verifikasi.
5. Masukkan kata sandi yang kuat untuk pengguna root Anda, konfirmasikan, lalu pilih Lanjutkan. AWSmengharuskan kata sandi Anda memenuhi ketentuan berikut:

   - Itu harus memiliki minimal 8 karakter dan maksimal 128 karakter.
   - Ini harus mencakup minimal tiga dari campuran tipe karakter berikut: huruf besar, huruf kecil, angka, dan! @ # $% ^ & * () <> [] {} | _+-= simbol.
   - Itu tidak boleh identik dengan Akun AWS nama atau alamat email Anda.

6. Pilih Bisnis atau Pribadi. Perbedaan antara opsi ini adalah informasi yang kami minta kepada Anda. Kedua jenis akun memiliki fitur dan fungsi yang sama.
7. Masukkan informasi bisnis atau pribadi Anda. Lihat rekomendasi di bagian Prasyarat tentang alamat email dan nomor telepon.
8. Baca dan terima Perjanjian AWS Pelanggan. Pastikan Anda membaca dan memahami ketentuan Perjanjian AWS Pelanggan.
9. Pilih Continue (Lanjutkan). Pada titik ini, Anda akan menerima pesan email untuk mengonfirmasi bahwa Anda Akun AWS siap digunakan. Anda dapat masuk ke akun baru Anda dengan

menggunakan alamat email dan kata sandi yang Anda berikan saat mendaftar. Namun, Anda tidak dapat menggunakan AWS layanan apa pun sampai Anda selesai mengaktifkan akun Anda.

10. Masukkan informasi tentang metode pembayaran Anda. Jika Anda ingin menggunakan alamat lain untuk tujuan penagihan, pilih Gunakan alamat baru.
11. Pilih Verifikasi dan Lanjutkan.
12. Masukkan kode negara atau wilayah Anda dari daftar, lalu masukkan nomor telepon tempat Anda dapat dihubungi dalam beberapa menit ke depan. Masukkan kode CAPTCHA, dan kirimkan.
13. Ketika sistem otomatis menghubungi Anda, masukkan PIN yang Anda terima dan kemudian kirimkan.
14. Pilih AWS Support paket Anda. Untuk deskripsi paket yang tersedia, lihat Membandingkan AWS Support paket.
15. Pilih Daftar lengkap. Halaman konfirmasi muncul yang menunjukkan bahwa akun Anda sedang diaktifkan.
16. Periksa folder email dan spam Anda untuk pesan email yang mengonfirmasi akun Anda telah diaktifkan. Aktivasi biasanya memakan waktu beberapa menit tetapi terkadang bisa memakan waktu hingga 24 jam.

    Setelah Anda menerima pesan aktivasi, Anda memiliki akses penuh ke semua AWS layanan.

> **Note**
>
> Jika Anda mengalami masalah dengan aktivasi akun, lihatthe section called “Masalah pembuatan akun”.

Langkah 2: Aktifkan MFA untuk pengguna root Anda

Kami sangat menyarankan Anda mengaktifkan MFA untuk pengguna root Anda. MFA secara dramatis menurunkan risiko seseorang mengakses akun Anda tanpa izin Anda.

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi Anda.

Untuk bantuan saat masuk menggunakan pengguna root, lihat Masuk ke pengguna root AWS Management Console sebagai pengguna root di Panduan Pengguna AWS Masuk.

2. Nyalakan MFA untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Langkah 3: Buat pengguna administrator

Karena Anda tidak dapat membatasi apa yang dapat dilakukan pengguna root, kami sangat menyarankan agar Anda tidak menggunakan pengguna root Anda untuk tugas apa pun yang tidak secara eksplisit memerlukan pengguna root. Sebagai gantinya, tetapkan akses administratif ke pengguna administratif di Pusat Identitas IAM, dan masuk sebagai pengguna administratif tersebut untuk melakukan tugas administratif harian Anda.

Untuk petunjuk, lihat Mengatur Akun AWS akses untuk pengguna administratif Pusat Identitas IAM di Panduan Pengguna Pusat Identitas IAM.

Topik terkait

- Untuk informasi tentang melindungi kredensial pengguna root Anda, lihat Mengamankan kredenal untuk pengguna root di Panduan Pengguna IAM.
- Untuk daftar tugas yang memerlukan pengguna root, lihat Tugas yang memerlukan kredensi pengguna root di Panduan Pengguna IAM.

Menggunakan Pengguna root akun AWS

> **Important**
>
> Siapa pun yang memiliki kredensi pengguna root untuk Anda Akun AWS memiliki akses tidak terbatas ke semua sumber daya di akun Anda, termasuk informasi penagihan.

Saat Anda membuatAkun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna root Akun AWS dan diakses dengan cara masuk menggunakan alamat email dan kata sandi yang Anda

gunakan saat membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari Anda. Lindungi kredensil pengguna root Anda dan gunakan untuk melakukan tugas-tugas yang hanya dapat dilakukan oleh pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensi pengguna root di Panduan Pengguna IAM.

Untuk menghindari penggunaan pengguna root untuk tugas sehari-hari, pelajari cara mengatur pengguna administratif AWS IAM Identity Center. Untuk rekomendasi keamanan pengguna root tambahan, lihat Praktik terbaik pengguna Root untuk Anda Akun AWS.

Anda dapat mengubah, atau mengatur ulang kata sandi pengguna root, dan membuat, atau menghapus kunci akses (ID kunci akses dan kunci akses rahasia) untuk pengguna root Anda. Untuk bantuan saat masuk menggunakan pengguna root, lihat Masuk ke pengguna root AWS Management Console sebagai pengguna root di Panduan Pengguna AWS Masuk.

KelolaAkun AWS

Bagian ini mencakup topik yang menjelaskan cara mengelolaAkun AWS.

> **Note**
>
> Jika AndaAkun AWSdibuat di India dengan menggunakanAmazon Internet Services Private Limited(AISPL), ada pertimbangan tambahan. Untuk informasi selengkapnya, lihat Mengelola akun di India.

Topik

- Buat mandiri Akun AWS
- Lihat Akun AWS pengidentifikasi
- Perbarui Akun AWS nama, alamat email, atau kata sandi untuk pengguna root
- Memahami mode operasi API
- PerbaruiAkun AWSinformasi kontak
- Perbarui pertanyaan tantangan keamanan
- Tentukan Wilayah AWS akun mana yang dapat digunakan
- Buat atau perbarui Akun AWS alias Anda
- Tagihan AndaAkun AWS
- Mengelola akun di India
- Tutup sebuah Akun AWS

Buat mandiri Akun AWS

Topik ini menjelaskan cara membuat standalone Akun AWS yang tidak dikelola olehAWS Organizations. Jika Anda ingin membuat akun yang merupakan bagian dari organisasi yang dikelola olehAWS Organizations, lihat Membuat akun anggota di organisasi Anda di Panduan AWS Organizations Pengguna.

Instruksi ini untuk membuat Akun AWS bagian luar India. Untuk membuat akun di India, lihatBuat sebuahAkun AWSdengan AISPL.

AWS Management Console

Untuk membuat Akun AWS

1. Buka halaman beranda Amazon Web Services.
2. Pilih Buat Akun AWS.

> **Note**
>
> Jika Anda masuk AWS baru-baru ini, opsi itu mungkin tidak ada. Sebagai gantinya, pilih Masuk ke Konsol. Kemudian, jika Buat yang baru Akun AWS masih tidak terlihat, pertama-tama pilih Masuk ke akun lain, lalu pilih Buat yang baru Akun AWS.

3. Masukkan informasi akun Anda, lalu pilih Verifikasi alamat email. Ini akan mengirimkan kode verifikasi ke alamat email yang Anda tentukan.

> **Important**
>
> Karena sifat kritis dari pengguna root akun, kami sangat menyarankan Anda menggunakan alamat email yang dapat diakses oleh grup, bukan hanya individu. Dengan begitu, jika orang yang mendaftar Akun AWS meninggalkan perusahaan, masih Akun AWS dapat digunakan karena alamat emailnya masih dapat diakses. Jika Anda kehilangan akses ke alamat email yang terkait denganAkun AWS, maka Anda tidak dapat memulihkan akses ke akun jika Anda kehilangan kata sandi.

4. Masukkan kode verifikasi Anda, lalu pilih Verifikasi.
5. Masukkan kata sandi yang kuat untuk pengguna root Anda, konfirmasikan, lalu pilih Lanjutkan. AWSmengharuskan kata sandi Anda memenuhi ketentuan berikut:
   - Itu harus memiliki minimal 8 karakter dan maksimal 128 karakter.
   - Ini harus mencakup minimal tiga dari campuran tipe karakter berikut: huruf besar, huruf kecil, angka, dan! @ # $% ^ & * () <> [] {} | _+-= simbol.
   - Itu tidak boleh identik dengan Akun AWS nama atau alamat email Anda.
6. Pilih Bisnis atau Pribadi. Akun pribadi dan akun bisnis memiliki fitur dan fungsi yang sama.
7. Masukkan informasi perusahaan atau pribadi Anda.

> **Important**
>
> Untuk bisnisAkun AWS, ini adalah praktik terbaik untuk masuk:
>
> - Nomor telepon perusahaan bukan nomor untuk telepon pribadi.
> - Alamat email dengan nama domain milik perusahaan atau organisasi yang akan menggunakan akun tersebut.
>
> Mengkonfigurasi pengguna root akun dengan alamat email individual atau nomor telepon pribadi dapat membuat akun Anda tidak aman.

8. Baca dan terima Perjanjian AWS Pelanggan. Pastikan Anda membaca dan memahami ketentuan Perjanjian AWS Pelanggan.
9. Pilih Continue (Lanjutkan). Pada titik ini, Anda akan menerima pesan email untuk mengonfirmasi bahwa Anda Akun AWS siap digunakan. Anda dapat masuk ke akun baru Anda dengan menggunakan alamat email dan kata sandi yang Anda berikan saat mendaftar. Namun, Anda tidak dapat menggunakan AWS layanan apa pun sampai Anda selesai mengaktifkan akun Anda.
10. Masukkan informasi tentang metode pembayaran Anda, lalu pilih Verifikasi dan Lanjutkan. Jika Anda ingin menggunakan alamat penagihan yang berbeda untuk informasi AWS penagihan Anda, pilih Gunakan alamat baru.

    Anda tidak dapat melanjutkan proses pendaftaran sampai Anda menambahkan metode pembayaran yang valid.
11. Masukkan kode negara atau wilayah Anda dari daftar, lalu masukkan nomor telepon tempat Anda dapat dihubungi dalam beberapa menit ke depan.
12. Masukkan kode yang ditampilkan di CAPTCHA, lalu kirimkan.
13. Ketika sistem otomatis menghubungi Anda, masukkan PIN yang Anda terima dan kemudian kirimkan.
14. Pilih salah satu AWS Support paket yang tersedia. Untuk penjelasan tentang paket Support yang tersedia dan manfaatnya, lihat Membandingkan AWS Support paket.
15. Pilih Daftar lengkap. Halaman konfirmasi muncul yang menunjukkan bahwa akun Anda sedang diaktifkan.

16. Periksa folder email dan spam Anda untuk pesan email yang mengonfirmasi akun Anda telah diaktifkan. Aktivasi biasanya memakan waktu beberapa menit tetapi terkadang bisa memakan waktu hingga 24 jam.

    Setelah Anda menerima pesan aktivasi, Anda memiliki akses penuh ke semua AWS layanan.

AWS CLI & SDKs

Anda dapat membuat akun anggota di organisasi yang dikelola AWS Organizations dengan menjalankan CreateAccountoperasi saat masuk ke akun manajemen organisasi.

Anda tidak dapat membuat mandiri Akun AWS di luar organisasi dengan menggunakan operasi AWS Command Line Interface (AWS CLI) atau AWS API.

Lihat Akun AWS pengidentifikasi

AWS menetapkan pengidentifikasi unik berikut untuk masing-masing: Akun AWS

Akun AWS ID

Angka 12 digit, seperti 012345678901, yang secara unik mengidentifikasi sebuah. Akun AWSBanyak AWS sumber daya menyertakan ID akun di Amazon Resource Names (ARN) mereka. Bagian ID akun membedakan sumber daya dalam satu akun dari sumber daya di akun lain. Jika Anda pengguna AWS Identity and Access Management (IAM), Anda dapat masuk AWS Management Console menggunakan ID akun atau alias akun. Meskipun ID akun, seperti informasi pengenal apa pun, harus digunakan dan dibagikan dengan hati-hati, ID tersebut tidak dianggap sebagai informasi rahasia, sensitif, atau rahasia.

ID pengguna kanonik

Pengidentifikasi alfa-numerik, seperti`79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be`, yang merupakan bentuk ID yang dikaburkan. Akun AWS Anda dapat menggunakan ID ini untuk mengidentifikasi Akun AWS saat memberikan akses lintas akun ke bucket dan objek menggunakan Amazon Simple Storage Service (Amazon S3). Anda dapat mengambil ID pengguna kanonik untuk Anda Akun AWS sebagai pengguna root atau pengguna IAM.

Anda harus diautentikasi dengan AWS untuk melihat pengidentifikasi ini.

> **Warning**
>
> Jangan berikan AWS kredensi Anda (termasuk kata sandi dan kunci akses) kepada pihak ketiga yang membutuhkan Akun AWS pengenal Anda untuk berbagi AWS sumber daya dengan Anda. Melakukan hal itu akan memberi mereka akses yang sama ke Akun AWS yang Anda miliki.

Temukan Akun AWS ID Anda

Anda dapat menemukan Akun AWS ID menggunakan salah satu AWS Management Console atau AWS Command Line Interface (AWS CLI). Di konsol, lokasi ID akun bergantung pada apakah Anda masuk sebagai pengguna root atau pengguna IAM. ID akun sama apakah Anda masuk sebagai pengguna root atau pengguna IAM.

Menemukan ID akun Anda sebagai pengguna root

AWS Management Console

Untuk menemukan Akun AWS ID Anda saat masuk sebagai pengguna root

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - Saat Anda masuk sebagai pengguna root, Anda tidak memerlukan izin IAM apa pun.

1. Di bilah navigasi di kanan atas, pilih nama atau nomor akun Anda, lalu pilih Kredensi keamanan.

   > **Tip**
   >
   > Jika Anda tidak melihat opsi Security credentials, Anda mungkin masuk sebagai pengguna federasi dengan peran IAM, bukan sebagai pengguna IAM. Dalam hal ini, cari entri Akun dan nomor ID akun di sebelahnya.

2. Di bagian Detail akun, nomor akun muncul di sebelah Akun AWS ID.

AWS CLI & SDKs

Untuk menemukan Akun AWS ID Anda menggunakan AWS CLI

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - Saat Anda menjalankan perintah sebagai pengguna root, Anda tidak memerlukan izin IAM apa pun.

Gunakan perintah get-caller-identity sebagai berikut.

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

Temukan ID akun Anda sebagai pengguna IAM

AWS Management Console

Untuk menemukan Akun AWS ID Anda saat masuk sebagai pengguna IAM

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - `account:GetAccountInformation`

1. Di bilah navigasi di kanan atas, pilih nama pengguna Anda dan kemudian pilih Kredensyal keamanan.

> **Tip**
>
> Jika Anda tidak melihat opsi Security credentials, Anda mungkin masuk sebagai pengguna federasi dengan peran IAM, bukan sebagai pengguna IAM. Dalam hal ini, cari entri Akun dan nomor ID akun di sebelahnya.

2. Di bagian atas halaman, di bawah Detail akun, nomor akun muncul di sebelah Akun AWS ID.

AWS CLI & SDKs

Untuk menemukan Akun AWS ID Anda menggunakan AWS CLI

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - Ketika Anda menjalankan perintah sebagai pengguna atau peran IAM, maka Anda harus memiliki:
>   - `sts:GetCallerIdentity`

Gunakan perintah get-caller-identity sebagai berikut.

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

Temukan ID pengguna kanonik untuk Anda Akun AWS

Anda dapat menemukan ID pengguna kanonik untuk Anda Akun AWS menggunakan AWS Management Console atau. AWS CLIID pengguna kanonik untuk akun khusus untuk akun Akun AWS itu. Anda dapat mengambil ID pengguna kanonik untuk Anda Akun AWS sebagai pengguna root, pengguna federasi, atau pengguna IAM.

Temukan ID kanonik sebagai pengguna root atau pengguna IAM

AWS Management Console

Untuk menemukan ID pengguna kanonik untuk akun Anda saat masuk ke konsol sebagai pengguna root atau pengguna IAM

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - Saat Anda menjalankan perintah sebagai pengguna root, Anda tidak memerlukan izin IAM apa pun.
> - Ketika Anda masuk sebagai pengguna IAM, maka Anda harus memiliki:
>   - `account:GetAccountInformation`

1. Masuk ke AWS Management Console sebagai pengguna root atau pengguna IAM.
2. Di bilah navigasi di kanan atas, pilih nama atau nomor akun Anda, lalu pilih Kredensi keamanan.

   > **Tip**
   >
   > Jika Anda tidak melihat opsi Security credentials, Anda mungkin masuk sebagai pengguna federasi dengan peran IAM, bukan sebagai pengguna IAM. Dalam hal ini, cari entri Akun dan nomor ID akun di sebelahnya.

3. Di bagian Detail akun, ID pengguna kanonik muncul di sebelah ID pengguna Canonical. Anda dapat menggunakan ID pengguna kanonik untuk mengonfigurasi daftar kontrol akses Amazon S3 (ACL).

AWS CLI & SDKs

Untuk menemukan ID pengguna kanonik menggunakan AWS CLI

Perintah yang sama AWS CLI dan API berfungsi untuk Pengguna root akun AWS, pengguna IAM, atau peran IAM.

Gunakan perintah list-buckets sebagai berikut.

```
$ aws s3api list-buckets \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Temukan ID kanonik sebagai pengguna federasi dengan peran IAM

AWS Management Console

Untuk menemukan ID kanonik untuk akun Anda saat masuk ke konsol sebagai pengguna gabungan dengan peran IAM

> **Izin minimum**
>
> - Anda harus memiliki izin untuk mendaftar dan melihat bucket Amazon S3.

1. Masuk ke AWS Management Console sebagai pengguna federasi dengan peran IAM.
2. Di konsol Amazon S3, pilih nama bucket untuk melihat detail tentang bucket.
3. Pilih tab Izin.
4. Di bagian Daftar kontrol akses, di bawah Pemilik Bucket, ID kanonik untuk Anda Akun AWS akan muncul.

AWS CLI & SDKs

Untuk menemukan ID pengguna kanonik menggunakan AWS CLI

Perintah yang sama AWS CLI dan API berfungsi untuk Pengguna root akun AWS, pengguna IAM, atau peran IAM.

Gunakan perintah list-buckets sebagai berikut.

```
$ aws s3api list-buckets \
    --query Owner.ID \
    --output text
```

```
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Perbarui Akun AWS nama, alamat email, atau kata sandi untuk pengguna root

Untuk mengedit Akun AWS nama Anda, atau untuk mengubah kata sandi atau alamat email pengguna root, lakukan langkah-langkah dalam prosedur berikut. Alamat email dan kata sandi ini adalah kredensi yang Anda gunakan untuk masuk sebagai. Pengguna root akun AWS

> **Note**
>
> Perubahan pada an Akun AWS dapat memakan waktu hingga empat jam untuk menyebar ke mana-mana.

AWS Management Console

Untuk mengedit Akun AWS nama Anda, kata sandi pengguna root, atau alamat email pengguna root

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - Anda harus masuk sebagaiPengguna root akun AWS, yang tidak memerlukan izin IAM tambahan. Anda tidak dapat melakukan langkah-langkah ini sebagai pengguna atau peran IAM.

1. Gunakan alamat email dan kata sandi Anda untuk masuk ke AWS Management Consolesebagai Akun AWS milik AndaPengguna root akun AWS.
2. Di sudut kanan atas konsol, pilih nama atau nomor akun Anda, lalu pilih Akun.
3. Pada halaman Akun, di samping Pengaturan akun, pilih Edit. Anda diminta untuk mengautentikasi ulang untuk tujuan keamanan.

> **Note**
>
> Jika Anda tidak melihat opsi Edit, kemungkinan Anda tidak masuk sebagai pengguna root untuk akun Anda. Anda tidak dapat mengubah setelan akun saat masuk sebagai pengguna atau peran IAM.

4. Pada halaman Perbarui pengaturan akun, pilih Edit di samping bidang yang ingin Anda perbarui.

   a. Untuk Nama — Pada halaman Perbarui nama akun Anda, di Nama akun baru, masukkan nama akun baru, lalu pilih Simpan perubahan.

   > **Note**
   >
   > Jika Anda tidak dapat mengubah Akun AWS nama, periksa apakah ada kebijakan kontrol layanan (SCP) AWS Organizations yang membatasi akses ke `account` atau diatur untuk menolak tindakan. `iam:UpdateAccountName`

   b. Untuk Email — Pada halaman Perbarui alamat email Anda, isi kolom untuk Alamat email baru, Konfirmasikan alamat email baru, dan konfirmasikan Kata Sandi Anda saat ini. Kemudian, pilih Simpan perubahan. Kode verifikasi dikirim ke alamat email baru Anda dari`no-reply@verify.signin.aws`. Pada halaman Verifikasi alamat email baru Anda, di bawah Kode verifikasi, masukkan kode yang Anda terima dari email, lalu pilih Simpan perubahan.

   > **Note**
   >
   > Diperlukan waktu hingga 5 menit agar kode verifikasi tiba. Jika Anda tidak melihat email di kotak masuk Anda, periksa folder spam dan sampah Anda.

   c. Untuk Kata Sandi — Pada halaman Perbarui kata sandi Anda, isi kolom untuk Kata Sandi Saat Ini, Kata sandi baru, dan Konfirmasi kata sandi baru. Kemudian, pilih Simpan perubahan. Untuk panduan tambahan termasuk praktik terbaik untuk menyetel kata sandi pengguna root, lihat Mengubah kata sandi untuk Panduan Pengguna IAM. Pengguna root akun AWS

5. Setelah Anda selesai membuat semua perubahan, memilih Selesai.

AWS CLI & SDKs

Tugas ini tidak didukung di AWS CLI atau oleh operasi API dari salah satu AWS SDK. Anda dapat melakukan tugas ini hanya dengan menggunakanAWS Management Console.

Memahami mode operasi API

Operasi API yang bekerja denganAkun AWSselalu bekerja di salah satu dari dua mode operasi:

- Konteks tunggal- mode ini digunakan ketika pengguna atau peran dalam akun mengakses atau mengubah atribut akun diakun yang sama. Mode konteks mandiri secara otomatis digunakan saat AndajangantermasukAccountIdparameter saat Anda memanggil salah satu Manajemen AkunAWS CLIatauAWSOperasi SDK.
- Konteks Organizations- mode ini digunakan ketika pengguna atau peran dalam satu akun dalam organisasi mengakses atau mengubah atribut akun di akun anggota yang berbeda di organisasi yang sama. Mode konteks organisasi secara otomatis digunakan saat AndaberbuattermasukAccountIdparameter saat Anda memanggil salah satu Manajemen AkunAWS CLIatauAWSOperasi SDK. Anda dapat memanggil operasi dalam mode ini hanya dari akun manajemen organisasi, atau akun admin yang didelegasikan untuk Manajemen Akun.

ParameterAWS CLIdanAWSOperasi SDK dapat bekerja baik dalam konteks mandiri atau organisasi.

- Jika AndajangantermasukAccountIdparameter, maka operasi berjalan dalam konteks mandiri dan secara otomatis menerapkan permintaan ke akun yang Anda gunakan untuk membuat permintaan. Ini benar apakah akun tersebut anggota sebuah organisasi atau tidak.
- Jika Anda menyertakanAccountIdparameter, maka operasi berjalan dalam konteks Organizations, dan operasi bekerja pada akun Organisasi yang ditentukan.
  - Jika akun yang memanggil operasi adalah akun manajemen atau akun admin yang didelegasikan untuk layanan Manajemen Akun, maka Anda dapat menentukan akun anggota organisasi tersebut diAccountIdparameter untuk memperbarui akun tertentu.
  - Satu-satunya akun dalam organisasi yang dapat memanggil salah satu operasi kontak alternatif dan menentukan nomor akunnya sendiri diAccountIdparameter adalah akun yang ditentukan sebagaiakun admin yang didelegasikanuntuk layanan Manajemen Akun. Akun lain, termasuk akun manajemen, menerimaAccessDeniedpengecualian.

- Jika Anda menjalankan operasi dalam mode mandiri, maka Anda harus diizinkan untuk menjalankan operasi dengan kebijakan IAM yang mencakup`Resource`elemen dari kedua`"*"`untuk memungkinkan semua sumber daya, atauARN yang menggunakan sintaks untuk akun tunggal.
- Jika Anda menjalankan operasi dalam mode organisasi, maka Anda harus diizinkan untuk menjalankan operasi dengan kebijakan IAM yang mencakup`Resource`elemen dari kedua`"*"`untuk memungkinkan semua sumber daya, atauARN yang menggunakan sintaks untuk akun anggota dalam organisasi.

Memberikan izin untuk memperbarui atribut akun

Seperti kebanyakanAWSoperasi, Anda memberikan izin untuk menambah, memperbarui, atau menghapus atribut akunAkun AWSdengan menggunakanKebijakan izin IAM. Saat Anda melampirkan kebijakan izin IAM ke prinsipal IAM (baik pengguna atau peran), Anda menentukan tindakan mana yang dapat dilakukan prinsipal pada sumber daya mana, dan dalam kondisi apa.

Berikut ini adalah beberapa pertimbangan khusus Manajemen Akun untuk membuat kebijakan izin.

Amazon Resource Name format untukAkun AWS

- ParameterAmazon Resource Name (ARN) AmazonuntukAkun AWSyang dapat Anda sertakan dalam`resource`elemen pernyataan kebijakan dibangun berbeda berdasarkan apakah akun yang ingin Anda referensi adalah akun mandiri atau akun yang ada di organisasi. Lihat bagian sebelumnya diMemahami mode operasi API.
  - Akun ARN untuk akun tunggal:

    ```
    arn:aws:account::{AccountId}:account
    ```

    Anda harus menggunakan format ini saat menjalankan operasi atribut akun dalam mode mandiri dengan tidak menyertakan`AccountID`parameter.
  - Akun ARN untuk akun anggota dalam organisasi:

    ```
    arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
    ```

    Anda harus menggunakan format ini saat menjalankan operasi atribut akun dalam mode organisasi dengan menyertakan`AccountID`parameter.

Kunci konteks untuk kebijakan IAM

Layanan Account Management juga menyediakan beberapaKunci ketentuan khusus layanan manajemen akunyang memberikan kontrol halus atas izin yang Anda berikan.

`account:AccountResourceOrgPaths`

Kunci konteks`account:AccountResourceOrgPaths`memungkinkan Anda menentukan jalur melalui hierarki organisasi Anda ke unit organisasi tertentu (OU). Hanya akun anggota yang terkandung oleh OU yang sesuai dengan kondisi tersebut. Contoh cuplikan berikut membatasi kebijakan untuk diterapkan hanya ke akun yang ada di salah satu dari dua OU yang ditentukan.

Karena`account:AccountResourceOrgPaths`adalah tipe string multi-nilai, Anda harus menggunakan`ForAnyValue`atau`ForAllValues`operator nilai ganda. Juga, perhatikan bahwa awalan pada kunci kondisi`account`, meskipun Anda merujuk jalur ke OU dalam sebuah organisasi.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgPaths": [
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*",
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/*"
        ]
    }
}
```

`account:AccountResourceOrgTags`

Kunci konteks`account:AccountResourceOrgTags`memungkinkan Anda mereferensikan tag yang dapat dilampirkan ke akun di organisasi. Tag adalah pasangan string kunci/nilai yang dapat Anda gunakan untuk mengkategorikan dan memberi label sumber daya di akun Anda. Untuk informasi lebih lanjut tentang penandaan, lihatEditor Tandadi dalamAWS Resource GroupsPanduan Pengguna. Untuk informasi tentang penggunaan tag sebagai bagian dari strategi kontrol akses berbasis atribut, lihatUntuk apa ABACAWSdi dalamPanduan Pengguna IAM. Cuplikan contoh berikut membatasi kebijakan untuk diterapkan hanya ke akun di organisasi yang memiliki tag dengan kunci`project`dan nilai keduanya`blue`atau`red`.

Karena`account:AccountResourceOrgTags`adalah tipe string multi-nilai, Anda harus menggunakan`ForAnyValue`atau`ForAllValues`operator nilai ganda. Juga, perhatikan bahwa awalan pada kunci kondisi`account`, meskipun Anda mereferensikan tag pada akun anggota organisasi.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgTags/project": [
            "blue",
            "red"
        ]
    }
}
```

> **Note**
>
> Anda dapat melampirkan tag hanya ke akun di organisasi. Anda tidak dapat melampirkan tag ke standaloneAkun AWS.

PerbaruiAkun AWSinformasi kontak

Anda dapat menyimpan informasi kontak tentangkontak akun utamauntuk AndaAkun AWS. Anda juga dapat menambahkan atau mengedit informasi kontak untuk yang berikutkontak akun alternatif:

- Penagihan- Kontak penagihan alternatif akan menerima pemberitahuan terkait penagihan, seperti pemberitahuan ketersediaan faktur.
- Operasi- Kontak operasi alternatif akan menerima pemberitahuan terkait operasi.
- Keamanan- Kontak keamanan alternatif akan menerima pemberitahuan terkait keamanan, termasuk pemberitahuan dariAWSTim Penyalahgunaan.

Topik

- Perbarui kontak alternatif untuk Anda Akun AWS
- Perbarui kontak utama untuk Anda Akun AWS

Perbarui kontak alternatif untuk Anda Akun AWS

Kontak alternatif memungkinkan AWS untuk menghubungi hingga tiga kontak alternatif yang terkait dengan akun. Kontak alternatif tidak harus menjadi orang tertentu. Sebagai gantinya, Anda dapat menambahkan daftar distribusi email jika Anda memiliki tim yang mengelola masalah terkait penagihan, operasi, dan keamanan. Ini adalah tambahan untuk alamat email yang terkait dengan

pengguna root akun. Kontak akun utama akan terus menerima semua komunikasi email yang dikirim ke email akun root.

Anda hanya dapat menentukan satu dari masing-masing jenis kontak berikut yang terkait dengan akun.

- Kontak penagihan
- Kontak operasi
- Kontak keamanan

Anda dapat menambahkan atau mengedit kontak alternatif secara berbeda, tergantung pada apakah akun berdiri sendiri atau tidak, atau bagian dari organisasi:

- Mandiri Akun AWS — Untuk Akun AWS tidak terkait dengan organisasi, Anda dapat memperbarui kontak alternatif Anda sendiri menggunakan Konsol AWS Manajemen, atau melalui AWS CLI & SDK. Untuk mempelajari cara melakukannya, lihat Memperbarui kontak Akun AWS alternatif mandiri.
- Akun AWSdalam organisasi — Untuk akun anggota yang merupakan bagian dari AWS organisasi, pengguna di akun manajemen atau akun admin yang didelegasikan dapat memperbarui akun anggota apa pun di organisasi secara terpusat dari AWS Organizations konsol, atau secara terprogram melalui CLI AWS & SDK. Untuk mempelajari cara melakukannya, lihat Memperbarui kontak Akun AWS alternatif di organisasi Anda.

Topik

- Persyaratan nomor telepon dan alamat email
- Perbarui kontak alternatif untuk mandiri Akun AWS
- Perbarui kontak alternatif untuk siapa pun Akun AWS di organisasi Anda
- akun: kunci AlternateContactTypes konteks

Persyaratan nomor telepon dan alamat email

Sebelum Anda melanjutkan dengan memperbarui informasi kontak alternatif akun Anda, kami sarankan Anda terlebih dahulu meninjau persyaratan berikut saat memasukkan nomor telepon dan alamat email.

- Nomor telepon hanya dapat berisi angka, spasi putih, dan karakter berikut:””. + - ( )

- Alamat email dapat mencapai 254 karakter dan dapat menyertakan karakter khusus berikut di bagian lokal alamat email selain yang alfanumerik standar: "". `+=.#|!&-_`

Perbarui kontak alternatif untuk mandiri Akun AWS

Untuk menambah atau mengedit kontak alternatif untuk mandiriAkun AWS, lakukan langkah-langkah dalam prosedur berikut. AWS Management ConsoleProsedur di bawah ini selalu berfungsi hanya dalam konteks mandiri. Anda dapat menggunakan AWS Management Console untuk mengakses atau mengubah hanya kontak alternatif di akun yang Anda gunakan untuk memanggil operasi.

AWS Management Console

Untuk menambah atau mengedit kontak alternatif untuk mandiri Akun AWS

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - `account:GetAlternateContact`(untuk melihat rincian kontak alternatif)
> - `account:PutAlternateContact`(untuk mengatur atau memperbarui kontak alternatif)
> - `account:DeleteAlternateContact`(untuk menghapus kontak alternatif)

1. Masuk ke AWS Management Consolesebagai pengguna IAM atau peran yang memiliki izin minimum.
2. Pilih nama akun Anda di kanan atas jendela, lalu pilih Akun.
3. Pada halaman Akun, gulir ke bawah ke Kontak alternatif, dan di sebelah kanan judul, pilih Edit.

> **Note**
>
> Jika Anda tidak melihat opsi Edit, kemungkinan Anda tidak masuk sebagai pengguna root untuk akun Anda atau sebagai seseorang yang memiliki izin minimum yang ditentukan di atas.

4. Ubah nilai di salah satu bidang yang tersedia.

> **Important**
>
> Untuk bisnisAkun AWS, itu adalah praktik terbaik untuk memasukkan nomor telepon perusahaan dan alamat email daripada satu milik individu.

5. Setelah Anda membuat semua perubahan, pilih Perbarui.

AWS CLI & SDKs

Anda dapat mengambil, memperbarui, atau menghapus informasi kontak alternatif dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **Catatan**
>
> - Untuk melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan di organisasi terhadap akun anggota, Anda harus mengaktifkan akses tepercaya untuk layanan Akun.

> **Izin minimum**
>
> Untuk setiap operasi, Anda harus memiliki izin yang memetakan ke operasi itu:
>
> - `GetAlternateContact`(untuk melihat rincian kontak alternatif)

- `PutAlternateContact`(untuk mengatur atau memperbarui kontak alternatif)
- `DeleteAlternateContact`(untuk menghapus kontak alternatif)

Jika Anda menggunakan izin individual ini, Anda dapat memberikan beberapa pengguna kemampuan untuk hanya membaca informasi kontak, dan memberi orang lain kemampuan untuk membaca dan menulis.

Example

Contoh berikut mengambil kontak alternatif Penagihan saat ini untuk akun pemanggil.

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

Contoh berikut menetapkan kontak alternatif Operasi baru untuk akun pemanggil.

```
$ aws account put-alternate-contact \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

Perintah ini tidak menghasilkan output jika berhasil.

Example

> **Note**
>
> Jika Anda melakukan beberapa `PutAlternateContact` operasi pada jenis kontak yang sama Akun AWS dan sama, yang pertama menambahkan kontak baru, dan semua panggilan berturut-turut ke jenis kontak yang sama Akun AWS dan memperbarui kontak yang ada.

Example

Contoh berikut menghapus kontak alternatif Keamanan untuk akun pemanggil.

```
$ aws account delete-alternate-contact \
    --alternate-contact-type=SECURITY
```

Perintah ini tidak menghasilkan output jika berhasil.

> **Note**
>
> Jika Anda mencoba menghapus kontak yang sama lebih dari sekali, yang pertama berhasil diam-diam. Semua upaya selanjutnya menghasilkan `ResourceNotFound` pengecualian.

Perbarui kontak alternatif untuk siapa pun Akun AWS di organisasi Anda

Untuk menambah atau mengedit rincian kontak alternatif untuk setiap orang Akun AWS di organisasi Anda, lakukan langkah-langkah dalam prosedur berikut.

Persyaratan

Untuk memperbarui kontak alternatif dengan AWS Organizations konsol, Anda perlu melakukan beberapa pengaturan awal:

- Organisasi Anda harus mengaktifkan semua fitur untuk mengelola pengaturan pada akun anggota Anda. Ini memungkinkan kontrol admin atas akun anggota. Ini diatur secara default saat Anda membuat organisasi. Jika organisasi Anda disetel ke penagihan gabungan saja, dan Anda ingin mengaktifkan semua fitur, lihat Mengaktifkan semua fitur di organisasi Anda.

- Anda perlu mengaktifkan akses tepercaya untuk layanan Manajemen AWS Akun. Untuk mengaturnya, lihat Mengaktifkan akses tepercaya untuk Manajemen AWS Akun.

> **Note**
>
> Kebijakan AWS Organizations terkelola `AWSOrganizationsReadOnlyAccess` atau `AWSOrganizationsFullAccess` diperbarui untuk memberikan izin mengakses API Manajemen AWS Akun sehingga Anda dapat mengakses data akun dari AWS Organizations konsol. Untuk melihat kebijakan terkelola yang diperbarui, lihat Kebijakan yang AWSdikelola Update to Organizations.

AWS Management Console

Untuk menambah atau mengedit kontak alternatif untuk siapa pun Akun AWS di organisasi Anda

1. Masuk ke AWS Organizationskonsol dengan kredenal akun manajemen organisasi.
2. Dari Akun AWS, pilih akun yang ingin Anda perbarui.
3. Pilih Info kontak, dan di bawah Kontak alternatif, cari jenis kontak: Kontak penagihan, Kontak keamanan, atau Kontak operasi.
4. Untuk menambahkan kontak baru, pilih Tambah, atau untuk memperbarui kontak yang ada pilih Edit.
5. Ubah nilai di salah satu bidang yang tersedia.

   > **Important**
   >
   > Untuk bisnisAkun AWS, itu adalah praktik terbaik untuk memasukkan nomor telepon perusahaan dan alamat email daripada satu milik individu.

6. Setelah Anda membuat semua perubahan, pilih Perbarui.

AWS CLI & SDKs

Anda dapat mengambil, memperbarui, atau menghapus informasi kontak alternatif dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **Catatan**
>
> - Untuk melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan di organisasi terhadap akun anggota, Anda harus mengaktifkan akses tepercaya untuk layanan Akun.
> - Anda tidak dapat mengakses akun di organisasi yang berbeda dari yang Anda gunakan untuk memanggil operasi.

> **Izin minimum**
>
> Untuk setiap operasi, Anda harus memiliki izin yang memetakan ke operasi itu:
>
> - `GetAlternateContact`(untuk melihat rincian kontak alternatif)
> - `PutAlternateContact`(untuk mengatur atau memperbarui kontak alternatif)
> - `DeleteAlternateContact`(untuk menghapus kontak alternatif)
>
> Jika Anda menggunakan izin individual ini, Anda dapat memberikan beberapa pengguna kemampuan untuk hanya membaca informasi kontak, dan memberi orang lain kemampuan untuk membaca dan menulis.

Example

Contoh berikut mengambil kontak alternatif Penagihan saat ini untuk akun pemanggil di organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account get-alternate-contact \
```

```
    --alternate-contact-type=BILLING \
    --account-id 123456789012
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

Contoh berikut menetapkan kontak alternatif Operasi untuk akun anggota tertentu dalam organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account put-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

Perintah ini tidak menghasilkan output jika berhasil.

> **Note**
>
> Jika Anda melakukan beberapa `PutAlternateContact` operasi pada jenis kontak yang sama Akun AWS dan sama, yang pertama menambahkan kontak baru, dan semua panggilan berturut-turut ke jenis kontak yang sama Akun AWS dan memperbarui kontak yang ada.

Example

Contoh berikut menghapus kontak alternatif Keamanan untuk akun anggota yang ditentukan dalam suatu organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account delete-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=SECURITY
```

Perintah ini tidak menghasilkan output jika berhasil.

Example

> **Note**
>
> Jika Anda mencoba menghapus kontak yang sama lebih dari sekali, yang pertama berhasil diam-diam. Semua upaya selanjutnya menghasilkan `ResourceNotFound` pengecualian.

akun: kunci AlternateContactTypes konteks

Anda dapat menggunakan kunci konteks `account:AlternateContactTypes` untuk menentukan mana dari tiga jenis penagihan yang diizinkan (atau ditolak) oleh kebijakan IAM. Misalnya, contoh kebijakan izin IAM berikut menggunakan kunci kondisi ini untuk mengizinkan prinsipal terlampir mengambil, tetapi tidak memodifikasi, hanya kontak `BILLING` alternatif untuk akun tertentu dalam organisasi.

Karena `account:AlternateContactTypes` adalah jenis string multi-nilai, Anda harus menggunakan `ForAnyValue`atau `ForAllValues` multi-nilai operator string.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "account:GetAlternateContact",
            "Resource": [
                "arn:aws:account::123456789012:account/o-aa111bb222/111111111111"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "account:AlternateContactTypes": [
                        "BILLING"
                    ]
```

```
                }
            }
        }
    ]
}
```

Perbarui kontak utama untuk Anda Akun AWS

Anda dapat memperbarui informasi kontak utama yang terkait dengan akun Anda, termasuk nama lengkap kontak Anda, nama perusahaan, alamat surat, nomor telepon, dan alamat situs web.

Anda mengedit kontak akun utama secara berbeda, tergantung pada apakah akun tersebut berdiri sendiri, atau bagian dari organisasi:

- Mandiri Akun AWS — Untuk Akun AWS tidak terkait dengan organisasi, Anda dapat memperbarui kontak akun utama Anda sendiri menggunakan Konsol AWS Manajemen, atau melalui AWS CLI & SDK. Untuk mempelajari cara melakukannya, lihat Memperbarui kontak Akun AWS utama mandiri.
- Akun AWSdalam organisasi — Untuk akun anggota yang merupakan bagian dari AWS organisasi, pengguna di akun manajemen atau akun admin yang didelegasikan dapat memperbarui akun anggota apa pun di organisasi secara terpusat dari AWS Organizations konsol, atau secara terprogram melalui CLI AWS & SDK. Untuk mempelajari cara melakukannya, lihat Memperbarui kontak Akun AWS utama di organisasi Anda.

Topik

- Persyaratan nomor telepon dan alamat email
- Perbarui kontak utama untuk mandiri Akun AWS
- Perbarui kontak utama untuk siapa pun Akun AWS di organisasi Anda

Persyaratan nomor telepon dan alamat email

Sebelum Anda melanjutkan dengan memperbarui informasi kontak utama akun Anda, kami sarankan Anda terlebih dahulu meninjau persyaratan berikut saat memasukkan nomor telepon dan alamat email.

- Nomor telepon hanya dapat berisi angka, spasi putih, dan karakter berikut:””. +-( )
- Nomor telepon harus dimulai dengan kode + dan negara dan tidak boleh memiliki nol di depan atau spasi tambahan setelah kode negara. Misalnya, +1 (AS/Kanada) atau +44 (Inggris).

- Nomor telepon harus menyertakan tanda hubung "-" antara kode area, kode pertukaran, dan kode lokal. Misalnya, +1 202-555-0179.

> **Note**
>
> Nomor telepon yang dimasukkan tanpa tanda hubung dapat mengakibatkan tidak dapat menerima panggilan selama proses verifikasi nomor telepon saat mengatur ulang perangkat MFA untuk pengguna root. Untuk informasi selengkapnya, lihat Bagaimana cara mengatur ulang perangkat MFA akun pengguna AWS root saya? .

- Untuk tujuan keamanan, nomor telepon harus mampu menerima SMS dariAWS. Nomor bebas pulsa tidak akan diterima karena sebagian besar tidak mendukung SMS.
- Untuk bisnisAkun AWS, itu adalah praktik terbaik untuk memasukkan nomor telepon perusahaan dan alamat email daripada satu milik individu. Mengkonfigurasi pengguna root akun dengan alamat email atau nomor telepon individu dapat membuat akun Anda sulit dipulihkan jika individu tersebut meninggalkan perusahaan.

Perbarui kontak utama untuk mandiri Akun AWS

Untuk mengedit detail kontak utama Anda untuk mandiriAkun AWS, lakukan langkah-langkah dalam prosedur berikut. AWS Management ConsoleProsedur di bawah ini selalu berfungsi hanya dalam konteks mandiri. Anda dapat menggunakan AWS Management Console untuk mengakses atau mengubah hanya informasi kontak utama dari akun yang Anda gunakan untuk memanggil operasi.

AWS Management Console

Untuk mengedit kontak utama Anda untuk mandiri Akun AWS

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - `account:GetContactInformation`(untuk melihat detail kontak utama)
> - `account:PutContactInformation`(untuk memperbarui detail kontak utama)

1. Masuk ke AWS Management Consolesebagai pengguna IAM atau peran yang memiliki izin minimum.
2. Pilih nama akun Anda di kanan atas jendela, lalu pilih Akun.
3. Gulir ke bawah ke bagian Informasi kontak, dan di sebelahnya pilih Edit.
4. Ubah nilai di salah satu bidang yang tersedia.
5. Setelah Anda membuat semua perubahan, pilih Perbarui.

AWS CLI & SDKs

Anda dapat mengambil, memperbarui, atau menghapus informasi kontak utama dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- GetContactInformation
- PutContactInformation

> **Catatan**
>
> - Untuk melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan di organisasi terhadap akun anggota, Anda harus mengaktifkan akses tepercaya untuk layanan Akun.

> **Izin minimum**
>
> Untuk setiap operasi, Anda harus memiliki izin yang memetakan ke operasi itu:
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`
>
> Jika Anda menggunakan izin individual ini, Anda dapat memberikan beberapa pengguna kemampuan untuk hanya membaca informasi kontak, dan memberi orang lain kemampuan untuk membaca dan menulis.

Example

Contoh berikut mengambil informasi kontak utama saat ini untuk akun pemanggil.

```
$ aws account get-contact-information
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

Contoh berikut menetapkan informasi kontak utama baru untuk akun pemanggil.

```
$ aws account put-contact-information --contact-information \
'{"AddressLine1": "123 Any Street", "City": "Seattle", "CompanyName": "Example Corp,
 Inc.", "CountryCode": "US", "DistrictOrCounty": "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Perintah ini tidak menghasilkan output jika berhasil.

Perbarui kontak utama untuk siapa pun Akun AWS di organisasi Anda

Untuk mengedit detail kontak utama Anda Akun AWS di organisasi Anda, lakukan langkah-langkah dalam prosedur berikut.

Persyaratan tambahan

Untuk memperbarui kontak utama dengan AWS Organizations konsol, Anda perlu melakukan beberapa pengaturan awal:

- Organisasi Anda harus mengaktifkan semua fitur untuk mengelola pengaturan pada akun anggota Anda. Ini memungkinkan kontrol admin atas akun anggota. Ini diatur secara default saat Anda membuat organisasi. Jika organisasi Anda disetel ke penagihan gabungan saja, dan Anda ingin mengaktifkan semua fitur, lihat Mengaktifkan semua fitur di organisasi Anda.
- Anda perlu mengaktifkan akses tepercaya untuk layanan Manajemen AWS Akun. Untuk mengaturnya, lihat Mengaktifkan akses tepercaya untuk Manajemen AWS Akun.

AWS Management Console

Untuk mengedit kontak utama Anda untuk setiap orang Akun AWS di organisasi Anda

1. Masuk ke AWS Organizationskonsol dengan kredenal akun manajemen organisasi.
2. Dari Akun AWS, pilih akun yang ingin Anda perbarui.
3. Pilih Info kontak, dan temukan Kontak utama,
4. Pilih Edit.
5. Ubah nilai di salah satu bidang yang tersedia.
6. Setelah Anda membuat semua perubahan, pilih Perbarui.

AWS CLI & SDKs

Anda dapat mengambil, memperbarui, atau menghapus informasi kontak utama dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- GetContactInformation
- PutContactInformation

> **Catatan**
>
> - Untuk melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan di organisasi terhadap akun anggota, Anda harus mengaktifkan akses tepercaya untuk layanan Akun.
> - Anda tidak dapat mengakses akun di organisasi yang berbeda dari yang Anda gunakan untuk memanggil operasi.

Izin minimum

Untuk setiap operasi, Anda harus memiliki izin yang memetakan ke operasi itu:

- `account:GetContactInformation`
- `account:PutContactInformation`

Jika Anda menggunakan izin individual ini, Anda dapat memberikan beberapa pengguna kemampuan untuk hanya membaca informasi kontak, dan memberi orang lain kemampuan untuk membaca dan menulis.

Example

Contoh berikut mengambil informasi kontak utama saat ini untuk akun anggota yang ditentukan dalam suatu organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account get-contact-information --account-id 123456789012
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

Contoh berikut menetapkan informasi kontak utama untuk akun anggota tertentu dalam organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account put-contact-information --account-id 123456789012 \
--contact-information '{"AddressLine1": "123 Any Street", "City": "Seattle",
 "CompanyName": "Example Corp, Inc.", "CountryCode": "US", "DistrictOrCounty":
 "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Perintah ini tidak menghasilkan output jika berhasil.

Perbarui pertanyaan tantangan keamanan

Pertanyaan tantangan keamanan adalah metode verifikasi yang digunakan sebelumnya untuk memverifikasi identitas dalam skenario pemulihan akun. Mereka kurang aman daripada bentuk verifikasi yang lebih modern, seperti otentikasi multi-faktor (MFA). Jika saat ini Anda memiliki pertanyaan tantangan keamanan yang aktif di AndaAkun AWS, AWS Support dapat menggunakannya untuk membantu mengautentikasi Anda sebagai pemilik akun.

> **Important**
>
> Mulai 5 Januari 2024, tidak AWS akan lagi mendukung pertanyaan tantangan keamanan untuk akun yang belum diaktifkan dan digunakan. Ini akan menghapus opsi untuk menambahkan pertanyaan tantangan keamanan baru dari halaman Akun di halamanAWS Management Console. Jika Anda telah menetapkan pertanyaan tantangan keamanan atau telah mengaturnya di akun manajemen di AWS Organisasi Anda, Anda dapat terus menggunakannya. Setelah 6 Januari 2025, tidak AWS akan lagi mendukung pertanyaan tantangan keamanan untuk semua pelanggan yang tersisa. Kami mendorong Anda untuk menambahkan MFA sebagai gantinya. Untuk informasi selengkapnya, lihat AWSAkun menghentikan penggunaan pertanyaan tantangan keamanan.

Untuk mengedit pertanyaan tantangan keamanan yang ada dan memberikan jawaban, lakukan langkah-langkah dalam prosedur berikut.

AWS Management Console

Untuk mengedit pertanyaan tantangan keamanan untuk Anda Akun AWS

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - `account:GetChallengeQuestions`(untuk melihat pertanyaan tantangan keamanan)
> - `account:PutChallangeQuestions`(untuk mengatur atau memperbarui pertanyaan tantangan keamanan)

1. Masuk ke AWS Management Consolesebagai Pengguna root akun AWS atau sebagai pengguna IAM atau peran yang memiliki izin minimum.
2. Pilih nama akun Anda di kanan atas jendela, lalu pilih Akun.
3. Gulir ke bawah ke bagian Pertanyaan tantangan keamanan dan pilih Edit.

   > **Note**
   >
   > Jika Anda tidak melihat opsi Edit, kemungkinan Anda tidak masuk sebagai pengguna root untuk akun Anda atau sebagai seseorang yang memiliki izin minimum yang ditentukan di atas.

4. Ubah nilai di salah satu bidang yang tersedia. Anda dapat memilih salah satu pertanyaan yang diberikan, dan kemudian memasukkan jawaban yang sesuai.
5. Setelah Anda menyelesaikan perubahan, pilih Perbarui.

AWS CLI & SDKs

Tugas ini tidak didukung di AWS CLI atau oleh operasi API dari salah satu AWS SDK. Anda dapat melakukan tugas ini hanya dengan menggunakanAWS Management Console.

Tentukan Wilayah AWS akun mana yang dapat digunakan

An Wilayah AWSadalah lokasi fisik di dunia di mana kami memiliki beberapa Availability Zone. Availability Zones terdiri dari satu atau lebih pusat AWS data diskrit, masing-masing dengan daya redundan, jaringan, dan konektivitas, ditempatkan di fasilitas terpisah. Ini berarti bahwa masing-masing Wilayah AWS secara fisik terisolasi dan independen dari Daerah lain. Wilayah memberikan toleransi kesalahan, stabilitas, dan ketahanan, dan juga dapat mengurangi latensi. Untuk peta Wilayah yang tersedia dan yang akan datang, lihat Wilayah dan Zona Ketersediaan.

Sumber daya yang Anda buat di satu Wilayah tidak ada di Wilayah lain kecuali Anda secara eksplisit menggunakan fitur replikasi yang ditawarkan oleh suatu layanan. AWS Misalnya, Amazon S3 dan Amazon EC2 mendukung replikasi lintas Wilayah. Beberapa layanan, seperti AWS Identity and Access Management (IAM), tidak memiliki sumber daya Regional.

Akun Anda menentukan Wilayah yang tersedia untuk Anda.

- An Akun AWS menyediakan beberapa Wilayah sehingga Anda dapat meluncurkan AWS sumber daya di lokasi yang memenuhi kebutuhan Anda. Misalnya, Anda mungkin ingin meluncurkan instans Amazon EC2 di Eropa agar lebih dekat dengan pelanggan Eropa Anda atau untuk memenuhi persyaratan hukum.
- Akun AWS GovCloud (AS-Barat) menyediakan akses ke Wilayah AWS GovCloud (AS-Barat) dan Wilayah AWS GovCloud (AS-Timur). Untuk informasi selengkapnya, lihat AWS GovCloud (US).
- Akun Amazon AWS (China) hanya menyediakan akses ke Wilayah Beijing dan Ningxia. Untuk informasi selengkapnya, lihat Amazon Web Services di Tiongkok.

Untuk daftar nama Wilayah dan kode yang sesuai, lihat Titik akhir Regional di Panduan Referensi AWS Umum. Untuk daftar AWS layanan yang didukung di setiap Wilayah (tanpa titik akhir), lihat Daftar Layanan AWS Regional.

> **Important**
>
> AWS merekomendasikan agar Anda menggunakan titik akhir regional AWS Security Token Service (AWS STS) alih-alih titik akhir global untuk mengurangi latensi. Token sesi dari AWS STS titik akhir regional berlaku di semua AWS Wilayah. Jika Anda menggunakan AWS STS titik akhir regional, Anda tidak perlu melakukan perubahan apa pun. Namun, token sesi dari AWS STS titik akhir global (https://sts.amazonaws.com) hanya valid jika Anda mengaktifkan, atau yang diaktifkan secara default. Wilayah AWS Jika Anda bermaksud mengaktifkan

Wilayah baru untuk akun Anda, Anda dapat menggunakan token sesi dari AWS STS titik akhir regional atau mengaktifkan AWS STS titik akhir global untuk mengeluarkan token sesi yang valid di semua. Wilayah AWS Token sesi yang valid di semua Wilayah lebih besar. Jika Anda menyimpan token sesi, token yang lebih besar ini dapat memengaruhi sistem Anda. Untuk informasi selengkapnya tentang cara kerja AWS STS titik akhir dengan AWS Wilayah, lihat Mengelola AWS STS di AWS Wilayah.

Topik

- Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah
- Mengaktifkan atau menonaktifkan Region untuk akun mandiri
- Mengaktifkan atau menonaktifkan Wilayah di organisasi Anda

Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah

Sebelum Anda mengaktifkan atau menonaktifkan Region, penting untuk mempertimbangkan hal berikut:

- Wilayah yang diperkenalkan sebelum 20 Maret 2019 diaktifkan secara default — AWS awalnya diaktifkan semua baru secara Wilayah AWS default, yang berarti Anda dapat segera mulai membuat dan mengelola sumber daya di Wilayah ini. Anda tidak dapat mengaktifkan atau menonaktifkan Wilayah yang diaktifkan secara default. Hari ini, saat AWS menambahkan Wilayah, Wilayah baru dinonaktifkan secara default. Jika Anda ingin pengguna dapat membuat dan mengelola sumber daya di Wilayah baru, Anda harus mengaktifkan Wilayah tersebut terlebih dahulu. Wilayah berikut dinonaktifkan secara default.

Nama	Kode
Afrika (Cape Town)	`af-south-1`
Asia Pasifik (Hong Kong)	`ap-east-1`
Asia Pasifik (Hyderabad)	`ap-south-2`
Asia Pasifik (Jakarta)	`ap-southeast-3`
Asia Pasifik (Melbourne)	`ap-southeast-4`

Nama	Kode
Kanada (Calgary)	`ca-west-1`
Eropa (Milan)	`eu-south-1`
Eropa (Spanyol)	`eu-south-2`
Eropa (Zürich)	`eu-central-2`
Israel (Tel Aviv)	`il-central-1`
Timur Tengah (Bahrain)	`me-south-1`
Middle East (UAE)	`me-central-1`

- Anda dapat menggunakan izin IAM untuk mengontrol akses ke Wilayah — AWS Identity and Access Management (IAM) mencakup empat izin yang memungkinkan Anda mengontrol pengguna mana yang dapat mengaktifkan, menonaktifkan, mendapatkan, dan mencantumkan Wilayah. Untuk informasi selengkapnya, lihat kebijakan tindakan Billing and Cost Management AWS Billing and Cost Management di Panduan Pengguna. Anda juga dapat menggunakan tombol `aws:RequestedRegion`kondisi untuk mengontrol akses ke Layanan AWS dalam file Wilayah AWS.
- Mengaktifkan Wilayah gratis — Tidak ada biaya untuk mengaktifkan Wilayah. Anda hanya dikenakan biaya untuk sumber daya yang Anda buat di Wilayah baru.
- Menonaktifkan Wilayah akan menonaktifkan akses IAM ke sumber daya di Wilayah — Jika Anda menonaktifkan Wilayah yang masih berisi AWS sumber daya, seperti instans Amazon Elastic Compute Cloud (Amazon EC2), Anda kehilangan akses IAM ke sumber daya di Wilayah tersebut. Misalnya, Anda tidak dapat menggunakan AWS Management Console untuk melihat atau mengubah konfigurasi instans EC2 apa pun di Wilayah yang dinonaktifkan.
- Biaya untuk sumber daya aktif berlanjut jika Anda menonaktifkan Wilayah — Jika Anda menonaktifkan Wilayah yang masih berisi AWS sumber daya, biaya untuk sumber daya tersebut (jika ada) terus bertambah dengan tarif standar. Misalnya, jika Anda nonaktifkan wilayah yang berisi instans Amazon EC2, Anda masih harus membayar biaya untuk instans tersebut meskipun instans tidak dapat diakses.
- Menonaktifkan Wilayah tidak selalu langsung terlihat — Layanan dan konsol mungkin terlihat sementara setelah menonaktifkan suatu wilayah. Menonaktifkan suatu Wilayah dapat memakan waktu beberapa menit hingga beberapa jam untuk diterapkan.

- Mengaktifkan Wilayah membutuhkan waktu beberapa menit hingga beberapa jam dalam beberapa kasus — Saat Anda mengaktifkan Wilayah, AWS lakukan tindakan untuk menyiapkan akun Anda di Wilayah tersebut, seperti mendistribusikan sumber daya IAM Anda ke Wilayah tersebut. Proses ini memakan waktu beberapa menit untuk sebagian besar akun, tetapi terkadang bisa memakan waktu beberapa jam. Anda tidak dapat menggunakan Wilayah sampai proses ini selesai.
- Organizations dapat memiliki 50 permintaan region-opt terbuka pada waktu tertentu di seluruh AWS organisasi — Akun manajemen dapat kapan saja memiliki 50 permintaan terbuka yang menunggu penyelesaian untuk organisasinya. Satu permintaan sama dengan mengaktifkan atau menonaktifkan satu wilayah tertentu untuk satu akun.
- Satu akun dapat memiliki 6 permintaan pilihan wilayah yang sedang berlangsung pada waktu tertentu - Satu permintaan sama dengan mengaktifkan atau menonaktifkan satu wilayah tertentu untuk satu akun.
- EventBridge Integrasi Amazon - Pelanggan dapat berlangganan notifikasi pembaruan status pilihan wilayah di. EventBridge EventBridgePemberitahuan akan dibuat untuk setiap perubahan status, memungkinkan pelanggan untuk mengotomatiskan alur kerja.
- Status Region-OPT Ekspresif - Karena sifat asinkron mengaktifkan/menonaktifkan wilayah keikutsertaan, ada empat status potensial untuk permintaan region-opt:
  - `ENABLING`
  - `DISABLING`
  - `ENABLED`
  - `DISABLED`

  Anda tidak dapat membatalkan opt-in atau opt-out ketika berada dalam salah satu atau `ENABLING` status. `DISABLING` Kalau tidak, `ConflictException` akan dilemparkan. Permintaan pilihan wilayah (Diaktifkan/Dinonaktifkan) yang telah selesai bergantung pada penyediaan layanan dasar utama. AWS Mungkin ada beberapa AWS layanan yang tidak akan segera dapat digunakan meskipun statusnya`ENABLED`.
- Integrasi penuh dengan AWS Organizations — Akun manajemen dapat memodifikasi atau membaca region-opt untuk akun anggota organisasi mana pun. AWS Akun anggota juga dapat membaca/menulis status wilayah mereka.

Mengaktifkan atau menonaktifkan Region untuk akun mandiri

Untuk memperbarui Wilayah mana yang dapat Anda Akun AWS akses, lakukan langkah-langkah dalam prosedur berikut. AWS Management Console Prosedur di bawah ini selalu berfungsi hanya

dalam konteks mandiri. Anda dapat menggunakan AWS Management Console untuk melihat atau memperbarui hanya Wilayah yang tersedia di akun yang Anda gunakan untuk memanggil operasi.

AWS Management Console

Untuk mengaktifkan atau menonaktifkan Region untuk standalone Akun AWS

> **Izin minimum**
>
> Untuk melakukan langkah-langkah dalam prosedur berikut, pengguna atau peran IAM harus memiliki izin berikut:
>
> - `account:ListRegions`(diperlukan untuk melihat daftar Wilayah AWS dan apakah mereka saat ini diaktifkan atau dinonaktifkan).
> - `account:EnableRegion`
> - `account:DisableRegion`

1. Masuk ke AWS Management Consolesebagai Pengguna root akun AWS atau sebagai pengguna IAM atau peran yang memiliki izin minimum.
2. Pilih nama akun Anda di kanan atas jendela, lalu pilih Akun.
3. Pada halaman Akun, gulir ke bawah ke bagian Wilayah AWS.

   > **Note**
   >
   > Anda mungkin diminta untuk menyetujui akses Anda ke informasi ini. AWS mengirimkan permintaan ke alamat email yang terkait dengan akun dan ke nomor telepon kontak utama. Pilih tautan dalam permintaan untuk membukanya di browser Anda, dan setujui aksesnya.

4. Di samping masing-masing Wilayah AWS dengan opsi di kolom Tindakan, pilih Aktifkan atau Nonaktifkan, tergantung pada apakah Anda ingin pengguna di akun Anda dapat membuat dan mengakses sumber daya di Wilayah tersebut.
5. Jika diminta, konfirmasikan pilihan Anda.
6. Setelah Anda membuat semua perubahan, pilih Perbarui.

AWS CLI & SDKs

Anda dapat mengaktifkan, menonaktifkan, membaca, dan mencantumkan status pilihan wilayah dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki izin yang memetakan ke operasi itu:
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

Jika Anda menggunakan izin individual ini, Anda dapat memberi beberapa pengguna kemampuan untuk hanya membaca informasi pilihan wilayah, dan memberi orang lain kemampuan untuk membaca dan menulis.

Contoh berikut memungkinkan wilayah untuk akun anggota yang ditentukan dalam suatu organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

Perhatikan bahwa Anda juga dapat menonaktifkan wilayah menggunakan perintah yang sama dan kemudian menggantinya `enable-region` dengan`disable-region`.

```
aws account enable-region --region-name af-south-1
```

Perintah ini tidak menghasilkan output jika berhasil.

Operasi ini asinkron. Perintah berikut akan memungkinkan Anda untuk melihat status permintaan terbaru.

```
aws account get-region-opt-status --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

Mengaktifkan atau menonaktifkan Wilayah di organisasi Anda

Untuk memperbarui Wilayah yang diaktifkan untuk akun anggota Anda AWS Organizations, lakukan langkah-langkah dalam prosedur berikut.

> **Note**
>
> Kebijakan AWS Organizations terkelola `AWSOrganizationsReadOnlyAccess` atau `AWSOrganizationsFullAccess` diperbarui untuk memberikan izin mengakses API Manajemen AWS Akun sehingga Anda dapat mengakses data akun dari AWS Organizations konsol. Untuk melihat kebijakan terkelola yang diperbarui, lihat Kebijakan yang AWS dikelola Update to Organizations.

> **Note**
>
> Sebelum Anda dapat melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan di organisasi untuk digunakan dengan akun anggota, Anda harus:
>
> - Aktifkan semua fitur di organisasi Anda untuk mengelola pengaturan di akun anggota Anda. Ini memungkinkan kontrol admin atas akun anggota. Ini diatur secara default saat Anda membuat organisasi. Jika organisasi Anda disetel ke penagihan gabungan saja, dan Anda ingin mengaktifkan semua fitur, lihat Mengaktifkan semua fitur di organisasi Anda.
> - Aktifkan akses tepercaya untuk layanan Manajemen AWS Akun. Untuk mengatur ini, lihatMengaktifkan akses tepercaya untuk Manajemen Akun AWS.

AWS Management Console

Untuk mengaktifkan atau menonaktifkan Wilayah di organisasi

1. Masuk ke AWS Organizations konsol dengan kredenal akun manajemen organisasi Anda.

2. Pada Akun AWShalaman, pilih akun yang ingin Anda perbarui.
3. Pilih tab Pengaturan akun.
4. Di bawah Wilayah, pilih Wilayah yang ingin Anda aktifkan atau nonaktifkan.
5. Pilih Tindakan, lalu pilih opsi Aktifkan atau Nonaktifkan.
6. Jika Anda memilih opsi Aktifkan, tinjau teks yang ditampilkan dan kemudian pilih Aktifkan wilayah.
7. Jika Anda memilih opsi Nonaktifkan, tinjau teks yang ditampilkan, ketik nonaktifkan untuk mengonfirmasi, lalu pilih Nonaktifkan wilayah.

AWS CLI & SDKs

Anda dapat mengaktifkan, menonaktifkan, membaca, dan mencantumkan status pilihan wilayah untuk akun anggota organisasi dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki izin yang memetakan ke operasi itu:
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

Jika Anda menggunakan izin individual ini, Anda dapat memberi beberapa pengguna kemampuan untuk hanya membaca informasi pilihan wilayah, dan memberi orang lain kemampuan untuk membaca dan menulis.

Contoh berikut memungkinkan wilayah untuk akun anggota yang ditentukan dalam suatu organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

Perhatikan bahwa Anda juga dapat menonaktifkan wilayah menggunakan perintah yang sama dan kemudian menggantinya `enable-region` dengan`disable-region`.

```
aws account enable-region --account-id 123456789012 --region-name af-south-1
```

Perintah ini tidak menghasilkan output jika berhasil.

> **Note**
>
> Sebuah organisasi hanya dapat memiliki hingga 20 permintaan wilayah pada waktu tertentu. Jika tidak, Anda akan menerima a`TooManyRequestsException`.

Operasi ini asinkron. Perintah berikut akan memungkinkan Anda untuk melihat status permintaan terbaru.

```
aws account get-region-opt-status --account-id 123456789012 --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

Buat atau perbarui Akun AWS alias Anda

Jika Anda ingin URL untuk pengguna IAM Anda berisi nama perusahaan Anda (atau easy-to-remember pengenal lain) alih-alih Akun AWS ID, Anda dapat membuat alias akun.

Untuk mempelajari cara membuat atau memperbarui alias akun, lihat Membuat, menghapus, dan mencantumkan Akun AWS alias di Panduan Pengguna IAM.

Tagihan AndaAkun AWS

Untuk prosedur dan tugas terkait penagihan yang terkait dengan AndaAkun AWS, lihat topik berikutAWS Billing and Cost ManagementPanduan Pengguna:

- Mengubah mata uang yang Anda gunakan untuk membayar tagihan
- Memperbarui dan menghapus nomor pendaftaran pajak
- Mengaktifkan warisan pengaturan pajak

Mengelola akun di India

Jika Anda mendaftar untuk yang baruAkun AWSdan pilih India untuk alamat kontak Anda, perjanjian pengguna Anda denganAmazon Internet Services Private Limited(AISPL), lokalAWSpenjual di India.AISPL mengelola penagihan Anda, dan total faktur Anda tercantum dalam rupee India (INR), bukan dolar AS (USD). Setelah Anda membuat akun dengan AISPL, Anda tidak dapat mengubah negara di informasi kontak Anda.

Jika Anda memilikiAkun AWSdengan alamat India, akun Anda baik denganAWSatau AISPL, tergantung kapan Anda membuka akun. Untuk mengetahui apakah akun Anda bersamaAWSatau AISPL, lihatDetermining which company your account is with. Jika Anda adalah pelanggan AWS yang sudah ada, Anda dapat terus menggunakan Akun AWS Anda. Anda juga dapat memilih untuk memiliki keduanyaAkun AWSdan akun AISPL, meskipun mereka tidak dapat dikonsolidasikan menjadi samaAWSorganisasi. Untuk informasi tentang mengelolaAkun AWS, lihatKelolaAkun AWS.

Jika akun Anda menggunakan AISPL, ikuti prosedur dalam topik ini untuk mengelola akun Anda. Topik ini menjelaskan cara mendaftar akun AISPL, mengedit informasi tentang akun AISPL Anda, dan menambahkan atau mengedit Nomor Akun Permanen (PAN) Anda.

Sebagai bagian dari proses verifikasi kartu kredit saat mendaftar, AISPL menagih kartu Anda sebesar 2 INR. AISPL mengembalikan 2 INR tersebut setelah verifikasi selesai. Anda mungkin akan dialihkan ke bank sebagai bagian dari proses verifikasi.

Topik

- Tentukan perusahaan mana akun Anda
- Buat sebuahAkun AWSdengan AISPL
- Kelola akun AISPL Anda

Tentukan perusahaan mana akun Anda

Layanan AWS yang disediakan baik oleh AWS dan AISPL. Gunakan prosedur ini untuk menentukan penjual mana yang memiliki akun Anda.

AWS Management Console

Untuk menentukan perusahaan mana akun Anda berada

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - Prosedur ini tidak memerlukan izin khusus.

1. BukaAWS Management ConsolepadaAWS Management Console.
2. Di footer halaman di bagian bawah halaman, lihat pemberitahuan hak cipta. Jika hak cipta adalah untuk Amazon Web Services, maka akun Anda adalah dengan AWS. Jika hak cipta adalah untuk Amazon Web Services Private Ltd, maka akun Anda adalah dengan AISPL.

AWS CLI & SDKs

Tugas ini tidak didukung diAWS CLIatau dengan operasi API dari salah satuAWSSDK. Anda dapat melakukan tugas ini hanya dengan menggunakanAWS Management Console.

Buat sebuahAkun AWSdengan AISPL

AISPL adalah penjual lokalAWSdi India. Gunakan prosedur berikut untuk daftar untuk akun AISPL jika alamat kontak Anda di India.

AWS Management Console

Untuk daftar untuk akun AISPL

> **Izin minimum**
>
> Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:
>
> - Karena operasi ini terjadi sebelum Anda memilikiAkun AWS, operasi ini tidak memerlukanAWSizin.

1. BukaAWS Management Console, dan kemudian pilihMasuk ke Konsol.
2. PadaMasukhalaman, masukkan alamat email yang ingin Anda gunakan.
3. Di bawah alamat email Anda, pilih Saya adalah pengguna baru, lalu memilih Masuk menggunakan server aman kami.
4. Untuk setiap bidang kredensi login, masukkan informasi Anda, lalu pilihBuat akun.
5. Untuk setiap bidang informasi kontak, masukkan informasi Anda.
6. Setelah Anda telah baca perjanjian pelanggan, pilih kotak centang syarat dan ketentuan, lalu memilih Buat Akun dan Lanjutkan.
7. Pada halaman Informasi Pembayaran, memasukkan metode pembayaran yang ingin Anda gunakan.
8. Di bawahInformasi PAN, pilihTidakjika Anda tidak memiliki Nomor Rekening Permanen (PAN) atau ingin menambahkannya nanti. Jika Anda memiliki PAN dan ingin menambahkannya sekarang, pilihya, dan di dalamPANCIbidang masukkan PAN Anda.
9. Memilih Verifikasi Kartu dan Lanjutkan. Anda harus memberikan CVV Anda sebagai bagian dari proses verifikasi. AISPL menagih kartu Anda sebesar 2 INR sebagai bagian dari proses verifikasi. AISPL mengembalikan 2 INR tersebut setelah verifikasi selesai.
10. UntukBerikan nomor telepon, masukkan nomor telepon Anda. Jika Anda memiliki ekstensi telepon, untukExt, masukkan ekstensi telepon Anda.
11. Memilih Hubungi Saya Sekarang. Setelah beberapa saat, pin empat digit akan muncul di layar Anda.
12. Terima panggilan otomatis dari AISPL. Pada keypad ponsel Anda, masukkan pin empat digit yang ditampilkan di layar Anda.
13. Setelah panggilan otomatis memverifikasi nomor kontak Anda, memilih Lanjutkan untuk Pilih Paket Support Anda.
14. Pada halaman Support Rencana Dukungan, pilih paket dukungan Anda, dan kemudian memilih Lanjutkan. Setelah metode pembayaran Anda diverifikasi dan akun Anda diaktifkan, Anda menerima pesan email yang mengonfirmasi aktivasi akun Anda.

AWS CLI & SDKs

Tugas ini tidak didukung diAWS CLIatau dengan operasi API dari salah satuAWSSDK. Anda dapat melakukan tugas ini hanya dengan menggunakanAWS Management Console.

Kelola akun AISPL Anda

Kecuali untuk tugas-tugas berikut, prosedur untuk mengelola akun Anda sama dengan akun yang dibuat di luar India. Lihat KelolaAkun AWS.

GunakanAWS Management Consoleuntuk melakukan tugas-tugas berikut:

- Menambah atau mengedit Nomor Rekening Permanen (PAN)
- Mengedit beberapa Nomor Akun Permanen (PAN)
- Mengedit beberapa Nomor Pajak Barang dan Jasa (GST)
- Melihat faktur pajak

Tutup sebuah Akun AWS

Jika Anda tidak lagi membutuhkannya Akun AWS, Anda dapat menutupnya kapan saja dengan mengikuti instruksi di bagian ini. Setelah Anda menutupnya, Anda dapat membukanya kembali dalam waktu 90 hari sejak Anda menutup akun. Jangka waktu antara hari Anda menutup akun dan ketika menutup akun AWS secara permanen disebut sebagai periode pasca-penutupan.

Apa yang perlu Anda ketahui sebelum menutup akun Anda

Sebelum menutup Anda Akun AWS, Anda harus mempertimbangkan hal berikut:

- Menutup akun Anda akan berfungsi sebagai pemberitahuan penghentian Perjanjian AWS Pelanggan untuk akun ini.
- Anda tidak perlu menghapus sumber daya Akun AWS sebelum menutupnya. Namun, kami sarankan Anda mencadangkan sumber daya atau data apa pun yang ingin Anda simpan. Untuk petunjuk tentang cara membuat cadangan sumber daya tertentu, lihat AWS dokumentasi yang sesuai untuk layanan tersebut.
- Anda dapat membuka kembali akun Anda selama periode pasca-penutupan. Biaya untuk layanan yang tersisa di akun Anda akan dimulai ulang jika Anda membukanya kembali. Anda juga tetap bertanggung jawab atas faktur yang belum dibayar dan Instans Cadangan dan Savings Plans yang belum dibayar.
- Anda tetap bertanggung jawab atas semua biaya dan biaya yang belum dibayar untuk layanan yang dikonsumsi sebelum penutupan akun. Anda akan menerima AWS tagihan pada bulan berikutnya setelah menutup akun Anda. Misalnya, jika Anda menutup akun Anda pada 15 Januari,

Anda akan menerima tagihan pada awal Februari untuk penggunaan yang terjadi dari 1 Januari hingga 15 Januari. Anda akan terus menerima faktur untuk Instans Cadangan dan Savings Plans setelah menutup akun Anda hingga habis masa berlakunya.

- Anda tidak akan lagi dapat mengakses AWS layanan yang sebelumnya tersedia di akun Anda. Namun, Anda dapat masuk dan mengakses penutupan Akun AWS selama periode pasca-penutupan hanya untuk melihat informasi penagihan sebelumnya, mengakses pengaturan akun, atau kontak. AWS Support
- Anda tidak dapat menggunakan alamat email yang sama yang terdaftar Akun AWS pada Anda pada saat penutupan sebagai email utama orang lain Akun AWS. Jika Anda ingin menggunakan alamat email yang sama untuk yang berbeda Akun AWS, kami sarankan untuk memperbaruinya sebelum penutupan. Lihat Perbarui Akun AWS nama, alamat email, atau kata sandi untuk pengguna root petunjuk tentang memperbarui alamat email Anda.
- Jika Anda telah mengaktifkan otentikasi multi-faktor (MFA) pada pengguna Akun AWS root Anda, atau mengonfigurasi perangkat MFA pada pengguna IAM, MFA tidak akan dihapus secara otomatis saat Anda menutup akun. Jika Anda memilih untuk membiarkan MFA dihidupkan selama 90 hari pasca-penutupan, jaga agar perangkat MFA tetap aktif hingga periode pasca-penutupan berakhir jika Anda perlu mengakses akun selama waktu itu. Catatan, perangkat token TOTP perangkat keras tidak dapat dikaitkan dengan pengguna lain setelah penutupan permanen akun Anda. Jika Anda ingin menggunakan token TOTP perangkat keras dengan pengguna lain nanti, Anda memiliki opsi untuk menonaktifkan perangkat MFA perangkat keras sebelum menutup akun. Perangkat MFA untuk pengguna IAM harus dihapus oleh administrator akun.

Pertimbangan tambahan untuk akun anggota

- Saat Anda menutup akun anggota, akun tersebut tidak akan dihapus dari organisasi sampai setelah periode pasca-penutupan. Selama periode pasca-penutupan, akun anggota tertutup masih diperhitungkan dalam kuota akun Anda di organisasi. Untuk menghindari jumlah akun terhadap kuota, lihat Menghapus akun anggota dari organisasi Anda sebelum menutupnya.
- Anda hanya dapat menutup 10% akun anggota dalam periode 30 hari bergulir. Kuota ini tidak terikat oleh bulan kalender, tetapi dimulai ketika Anda menutup akun. Dalam 30 hari sejak penutupan akun awal, Anda tidak dapat melebihi batas penutupan akun 10%. Penutupan akun minimum adalah 10 dan penutupan akun maksimum adalah 1000, bahkan jika 10% akun melebihi 1000. Untuk informasi selengkapnya tentang kuota Organizations, lihat Kuota untuk. AWS Organizations

- Jika Anda menggunakan AWS Control Tower, Anda harus membatalkan kelola akun anggota sebelum mencoba menutup akun. Lihat Membatalkan kelola akun anggota di Panduan Pengguna AWS Control Tower.

Pertimbangan khusus layanan

- AWS Marketplace langganan tidak dibatalkan secara otomatis pada penutupan akun. Jika Anda memiliki langganan, pertama-tama hentikan semua instance perangkat lunak Anda di langganan. Kemudian, buka halaman Kelola langganan AWS Marketplace konsol dan batalkan langganan Anda.
- Domain yang terdaftar dengan Route 53 tidak dihapus secara otomatis. Sebelum Anda menutup Akun AWS, Anda memiliki empat opsi:
  - Anda dapat menonaktifkan perpanjangan otomatis, dan domain secara otomatis dihapus ketika periode pendaftaran berakhir. Untuk informasi selengkapnya, lihat, Mengaktifkan atau Nonaktifkan Perpanjangan Otomatis untuk Domain dalam Panduan Developer Amazon Route 53.
  - Anda dapat transfer domain ke Akun AWS lain. Untuk informasi selengkapnya, lihat Transfer Domain ke Akun AWS yang Berbeda.
  - Anda dapat transfer domain ke pendaftar domain lain. Untuk informasi selengkapnya, lihat, Transfer Domain dari Route 53 ke Registrar Lain.
  - Jika Anda sudah menutup akun Anda, Anda dapat membuka kasing dengan bantuan mentransfer domain. AWS Support

Cara menutup akun Anda

Anda dapat menutup Anda Akun AWS menggunakan prosedur berikut. Perhatikan, bahwa ada panduan berbeda yang disediakan di setiap tab tergantung pada jenis akun [mandiri, anggota, manajemen, dan AWS GovCloud (US)] yang ingin Anda tutup.

Jika Anda mengalami masalah apa pun selama proses penutupan akun, lihatMemecahkan masalah dengan penutupan Akun AWS.

Standalone account

Akun mandiri adalah akun yang dikelola secara individual yang bukan merupakan bagian dari. AWS Organizations

Untuk menutup akun mandiri dari halaman Akun

1. Masuk ke AWS Management Console sebagai pengguna root Akun AWS yang ingin Anda tutup. Anda tidak dapat menutup akun saat masuk sebagai pengguna atau peran IAM.
2. Pada bilah navigasi di sudut kanan atas, pilih nama atau nomor akun Anda, lalu pilih Akun.
3. Pada halaman Akun, gulir ke bagian bawah halaman ke bagian Tutup akun. Baca dan pastikan Anda memahami proses penutupan akun.
4. Pilih tombol Tutup akun untuk memulai proses penutupan akun.
5. Dalam beberapa menit, Anda akan menerima konfirmasi email bahwa akun Anda telah ditutup.

> **Note**
>
> Tugas ini tidak didukung di AWS CLI atau oleh operasi API dari salah satu AWS SDK. Anda dapat melakukan tugas ini hanya dengan menggunakan AWS Management Console.

Member account

Akun anggota Akun AWS adalah bagian dari AWS Organizations.

Untuk menutup akun anggota dari AWS Organizations konsol

1. Masuk ke konsol AWS Organizations tersebut.
2. Pada Akun AWShalaman, temukan dan pilih nama akun anggota yang ingin Anda tutup. Anda dapat menavigasi hierarki OU, atau melihat daftar datar akun tanpa struktur OU.
3. Pilih Tutup di sebelah nama akun di bagian atas halaman. Organizations dalam mode penagihan Konsolidasi tidak akan dapat melihat tombol Tutup di konsol. Untuk menutup akun dalam mode penagihan konsolidasi, Anda harus mengikuti langkah-langkah di tab Akun mandiri.
4. Pilih setiap kotak centang untuk mengetahui semua laporan penutupan akun yang diperlukan.
5. Masukkan ID akun anggota lalu pilih Tutup akun.

Untuk menutup akun anggota dari halaman Akun

Secara opsional, Anda dapat menutup akun AWS anggota langsung dari halaman Akun di. AWS Management Console Untuk step-by-step panduan, ikuti petunjuk di tab Akun mandiri.

Untuk menutup akun anggota menggunakan AWS CLI dan SDK

Untuk petunjuk tentang cara menutup akun anggota menggunakan AWS CLI dan SDK, lihat Menutup akun anggota di organisasi Anda di Panduan AWS Organizations Pengguna.

Management account

Akun manajemen adalah akun Akun AWS yang bertindak sebagai akun induk atau root untuk AWS Organizations.

> **Note**
>
> Anda tidak dapat menutup akun manajemen langsung dari AWS Organizations konsol.

Untuk menutup akun manajemen dari halaman Akun

1. Masuk ke AWS Management Console sebagai pengguna root untuk akun manajemen yang ingin Anda tutup. Anda tidak dapat menutup akun saat masuk sebagai pengguna atau peran IAM.
2. Verifikasi bahwa tidak ada akun anggota aktif yang tersisa di organisasi Anda. Untuk melakukan ini, buka AWS Organizations konsol, dan pastikan semua akun anggota ditampilkan di `Suspended` sebelah nama akun mereka. Jika Anda memiliki akun anggota yang masih aktif, Anda harus mengikuti panduan penutupan akun yang disediakan di tab Akun Anggota sebelum Anda dapat melanjutkan ke langkah berikutnya.
3. Pada bilah navigasi di sudut kanan atas, pilih nama atau nomor akun Anda, lalu pilih Akun.
4. Pada halaman Akun, gulir ke bagian bawah halaman ke bagian Tutup akun. Baca dan pastikan Anda memahami proses penutupan akun.
5. Pilih tombol Tutup akun untuk memulai proses penutupan akun.
6. Dalam beberapa menit, Anda akan menerima konfirmasi email bahwa akun Anda telah ditutup.

> **Note**
>
> Tugas ini tidak didukung di AWS CLI atau oleh operasi API dari salah satu AWS SDK. Anda dapat melakukan tugas ini hanya dengan menggunakan AWS Management Console.

AWS GovCloud (US) account

AWS GovCloud (US) Akun selalu ditautkan ke satu standar Akun AWS untuk tujuan penagihan dan pembayaran.

Untuk menutup AWS GovCloud (US) akun

Jika Anda memiliki akun Akun AWS yang ditautkan ke AWS GovCloud (US) akun, Anda harus menutup akun standar sebelum menutup AWS GovCloud (US) akun. Untuk detail selengkapnya, termasuk cara mencadangkan data dan menghindari AWS GovCloud (US) tagihan yang tidak diinginkan, lihat Menutup AWS GovCloud (US) akun di AWS GovCloud (US) Panduan Pengguna.

Apa yang diharapkan setelah Anda menutup akun Anda

Segera setelah Anda menutup akun Anda, hal berikut akan terjadi:

- Anda akan menerima email yang mengonfirmasi penutupan akun ke alamat email pengguna root. Jika Anda tidak menerima email ini dalam beberapa jam, lihatMemecahkan masalah dengan penutupan Akun AWS.
- Setiap akun anggota yang Anda tutup akan menampilkan `SUSPENDED` label di sebelah nama akunnya di AWS Organizations konsol.
- Jika Anda telah memberikan izin untuk mengakses layanan di akun Anda Akun AWS ke akun lain, permintaan akses apa pun yang dibuat dari akun tersebut akan gagal setelah penutupan akun. Jika Anda membuka kembali Akun AWS, orang lain Akun AWS dapat kembali mengakses AWS layanan dan sumber daya akun Anda jika Anda memberikan izin yang diperlukan kepada mereka.

Periode pasca penutupan

Periode pasca-penutupan mengacu pada lamanya waktu antara hari Anda menutup akun Anda dan ketika menutup akun Anda AWS secara permanen. Akun AWS Periode pasca-penutupan adalah

90 hari. Selama periode pasca-penutupan, Anda dapat mengakses konten dan AWS layanan Anda hanya dengan membuka kembali akun Anda. Setelah periode pasca-penutupan, tutup AWS secara permanen Akun AWS, dan Anda tidak dapat lagi membukanya kembali. AWS juga akan menghapus konten dan sumber daya apa pun di akun Anda. Setelah akun ditutup secara permanen, Akun AWS ID-nya tidak akan pernah dapat digunakan kembali.

Membuka kembali Anda Akun AWS

Akun Anda akan ditutup secara permanen dalam 90 hari, setelah itu Anda tidak akan dapat membuka kembali akun Anda dan AWS akan menghapus konten yang tersisa di akun Anda. Untuk membuka kembali akun Anda sebelum ditutup secara permanen, (1) Anda harus menghubungi AWS Supportsesegera mungkin, dan (2) kami harus menerima pembayaran penuh dari saldo terutang, termasuk memberikan informasi yang diperlukan sebagaimana ditentukan pada faktur, dalam waktu 60 hari sejak tanggal penutupan akun.

Menggunakan Manajemen AWS Akun di organisasi Anda

AWS Organizationsadalah AWS layanan yang dapat Anda gunakan untuk mengelola Anda Akun AWS sebagai grup. Ini menyediakan fitur seperti penagihan konsolidasi, di mana semua tagihan akun Anda dikelompokkan bersama dan ditangani oleh satu pembayar. Anda juga dapat mengelola keamanan organisasi secara terpusat dengan menggunakan kontrol berbasis kebijakan. Untuk informasi selengkapnya tentang AWS Organizations, lihat AWS OrganizationsPanduan Pengguna .

Akses tepercaya

Saat Anda menggunakan AWS Organizations untuk mengelola akun Anda sebagai grup, sebagian besar tugas administratif untuk organisasi hanya dapat dilakukan oleh akun manajemen organisasi. Secara default, ini hanya mencakup operasi yang terkait dengan pengelolaan organisasi itu sendiri. Anda dapat memperluas fungsionalitas tambahan ini ke AWS layanan lain dengan mengaktifkan akses tepercaya antara Organisasi dan layanan tersebut. Akses tepercaya memberikan izin ke AWS layanan yang ditentukan untuk mengakses informasi tentang organisasi dan akun yang dikandungnya. Saat Anda mengaktifkan akses tepercaya untuk Manajemen Akun, layanan Manajemen Akun memberikan izin kepada Organisasi dan akun manajemennya untuk mengakses metadata, seperti informasi kontak utama atau alternatif, untuk semua akun anggota organisasi.

Untuk informasi selengkapnya, lihat Mengaktifkan akses tepercaya untuk Manajemen Akun AWS.

Admin yang didelegasikan

Setelah mengaktifkan akses tepercaya, Anda juga dapat memilih untuk menunjuk salah satu akun anggota Anda sebagai akun admin yang didelegasikan untuk AWS Manajemen Akun. Hal ini memungkinkan akun admin yang didelegasikan untuk melakukan tugas manajemen metadata Manajemen Akun yang sama untuk akun anggota di organisasi Anda yang sebelumnya hanya dapat dilakukan oleh akun manajemen. Akun admin yang didelegasikan hanya dapat mengakses tugas manajemen untuk layanan Manajemen Akun. Akun admin yang didelegasikan tidak memiliki semua akses administratif ke organisasi yang dimiliki akun manajemen.

Untuk informasi selengkapnya, lihat Mengaktifkan akun admin yang didelegasikan untukAWSPengelolaan Akun.

Kebijakan kontrol layanan

Ketika Anda Akun AWS adalah bagian dari organisasi yang dikelola olehAWS Organizations, maka administrator organisasi dapat menerapkan kebijakan kontrol layanan (SCP) yang dapat membatasi

apa yang dapat dilakukan oleh prinsipal di akun anggota. SCP tidak pernah memberikan izin; sebagai gantinya, ini adalah filter yang membatasi izin apa yang dapat digunakan oleh akun anggota. Pengguna atau peran (prinsipal) dalam akun anggota hanya dapat melakukan operasi yang berada di persimpangan dari apa yang diizinkan oleh SCP yang berlaku untuk akun dan kebijakan izin IAM yang melekat pada prinsipal. Misalnya, Anda dapat menggunakan SCP untuk mencegah pokok apa pun di akun memodifikasi kontak alternatif akun mereka sendiri.

Misalnya SCP yang berlaku untukAkun AWS, lihatMembatasi aksesAWS Organizationskebijakan kontrol layanan.

Mengaktifkan akses tepercaya untuk Manajemen Akun AWS

Mengaktifkan akses tepercaya untuk Manajemen AWS Akun memungkinkan administrator akun manajemen untuk mengubah informasi dan metadata (misalnya, detail kontak primer atau alternatif) khusus untuk setiap akun anggota di. AWS Organizations Untuk informasi selengkapnya, lihat Manajemen AWS Akun dan AWS Organizations di Panduan AWS Organizations Pengguna. Untuk informasi umum tentang cara kerja akses tepercaya, lihat Menggunakan AWS Organizations dengan AWS layanan lain.

Setelah akses tepercaya diaktifkan, Anda dapat menggunakan `accountID` parameter dalam operasi API Manajemen Akun yang mendukungnya. Anda dapat menggunakan parameter ini dengan sukses hanya jika Anda memanggil operasi menggunakan kredensi dari akun manajemen, atau dari akun admin yang didelegasikan untuk organisasi Anda jika Anda mengaktifkannya. Untuk informasi selengkapnya, lihat Mengaktifkan akun admin yang didelegasikan untukAWSPengelolaan Akun.

Gunakan prosedur berikut untuk mengaktifkan akses tepercaya untuk Manajemen Akun di organisasi Anda.

Izin minimum

Untuk melakukan tugas-tugas ini, Anda harus memenuhi persyaratan berikut:

- Anda dapat melakukan ini hanya dari akun manajemen organisasi.
- Organisasi Anda harus mengaktifkan semua fitur.

AWS Management Console

Untuk mengaktifkan akses tepercaya untuk Manajemen AWS Akun

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pilih Layanan di panel navigasi.
3. Pilih Manajemen AWS Akun dalam daftar layanan.
4. Pilih Aktifkan akses terpercaya.
5. Di kotak dialog Aktifkan akses tepercaya untuk Manajemen AWS Akun, ketik aktifkan untuk mengonfirmasi, lalu pilih Aktifkan akses tepercaya.

AWS CLI & SDKs

Untuk mengaktifkan akses tepercaya untuk Manajemen AWS Akun

Setelah menjalankan perintah berikut, Anda dapat menggunakan kredensi dari akun manajemen organisasi untuk memanggil operasi API Manajemen Akun yang menggunakan `--accountId` parameter untuk mereferensikan akun anggota di organisasi.

- AWS CLI: enable-aws-service-access

  Contoh berikut memungkinkan akses tepercaya untuk Manajemen AWS Akun di organisasi akun panggilan.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output jika berhasil.

Mengaktifkan akun admin yang didelegasikan untukAWSPengelolaan Akun

Akun admin yang didelegasikan dapat menghubungiAWSOperasi API Manajemen untuk akun anggota lainnya di organisasi. Untuk menetapkan akun anggota di organisasi Anda sebagai akun admin yang didelegasikan, gunakan prosedur berikut.

Izin minimum

Untuk melakukan tugas-tugas ini, Anda harus memenuhi persyaratan berikut:

- Anda dapat melakukan ini hanya dari akun manajemen organisasi.
- Organisasi Anda harus mengaktifkan semua fitur.
- Anda harus memilikimengaktifkan akses tepercaya untuk Manajemen Akun di organisasi Anda.

Setelah Anda menentukan akun admin yang didelegasikan untuk organisasi Anda, pengguna dan peran di akun tersebut dapat menghubungiAWS CLIdanAWSOperasi SDK di`account`namespace yang dapat bekerja dalam mode Organizations dengan mendukung opsional`AccountId`parameter.

AWS Management Console

Tugas ini tidak didukung diAWSKonsol manajemen Manajemen Akun. Anda dapat melakukan tugas ini hanya dengan menggunakanAWS CLIatau operasi API dari salah satuAWSSDK.

AWS CLI & SDKs

Untuk mendaftarkan akun admin yang didelegasikan untuk layanan Manajemen Akun

Anda dapat menggunakan perintah berikut untuk mengaktifkan admin yang didelegasikan untuk layanan Manajemen Akun.

Anda harus menentukan prinsipal layanan berikut:

```
account.amazonaws.com
```

- AWS CLI:mendaftar-delegasi-administrator

  Contoh berikut mendaftarkan akun anggota organisasi sebagai admin yang didelegasikan untuk layanan Manajemen Akun.

  ```
  $ aws organizations register-delegated-administrator \
      --account-id 123456789012 \
      --service-principal account.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output jika berhasil.

Setelah menjalankan perintah ini, Anda dapat menggunakan kredensia dari akun 123456789012 untuk memanggil Manajemen AkunAWS CLIdan operasi SDK API yang menggunakan`--account-id`parameter untuk referensi akun anggota dalam suatu organisasi.

Membatasi aksesAWS Organizationskebijakan kontrol layanan

Topik ini menyajikan contoh yang menunjukkan cara Anda dapat menggunakan kebijakan kontrol layanan (SCP) untuk membatasi apa yang dapat dilakukan pengguna dan peran yang ada dalam akun yang ada dalam organisasi. Untuk informasi selengkapnya tentang kebijakan kontrol layanan, lihat topik-topik berikut.AWS OrganizationsPanduan Pengguna:

- Membuat SCP
- Melampirkan SCP ke OU dan akun
- Strategi untuk SCP
- Sintaks kebijakan SCP

Example Contoh 1: Mencegah akun memodifikasi kontak alternatif mereka sendiri

Contoh berikut menyangkal`PutAlternateContact`dan`DeleteAlternateContact`Operasi API agar tidak dipanggil oleh akun anggota mana pun dimode akun mandiri. Ini mencegah pokok apa pun di akun yang terpengaruh mengubah kontak alternatif mereka sendiri.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "arn:aws:account::*:account" ]
        }
    ]
}
```

Example Contoh 2: Mencegah akun anggota memodifikasi kontak alternatif untuk akun anggota lain di organisasi

Contoh berikut menggeneralisasi`Resource`elemen untuk “*”, yang berarti bahwa hal itu berlaku untuk keduapermintaan mode mandiri dan permintaan mode organisasi. Ini berarti bahwa bahkan akun admin yang didelegasikan untuk Manajemen Akun, jika SCP berlaku untuk itu, diblokir dari mengubah kontak alternatif apa pun untuk akun apa pun di organisasi.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "*" ]
        }
    ]
}
```

Example Contoh 3: Mencegah akun anggota di OU dari memodifikasi kontak alternatifnya sendiri

Contoh berikut SCP mencakup kondisi yang membandingkan jalur organisasi akun dengan daftar dua OU. Ini menghasilkan pemblokiran kepala sekolah di akun apa pun di OU yang ditentukan dari memodifikasi kontak alternatif mereka sendiri.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": "account:PutAlternateContact",
            "Resource": [
                "arn:aws:account::*:account"
            ],
            "Condition": {
                "ForAnyValue:StringLike": {
                    "account:AccountResourceOrgPath": [
```

```
                        "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/",
                        "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/"
                    ]
                }
            }
    ]
}
```

Keamanan diAWSPengelolaan Akun

Keamanan cloud di AWS merupakan prioritas tertinggi. Sebagai pelanggan AWS, Anda akan mendapatkan manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan dari cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan AWS di Cloud AWS Cloud. AWS juga menyediakan layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga menguji dan memverifikasi secara berkala efektivitas keamanan kami sebagai bagian dari Program Kepatuhan AWS. Untuk mempelajari program kepatuhan yang berlaku di Pengelolaan Akun, lihatLayanan AWSdalam lingkup dengan program kepatuhan.
- Keamanan dalam cloud – Tanggung jawab Anda ditentukan oleh layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, mencakup kepekaan data Anda, persyaratan perusahaan, serta peraturan perundangan yang berlaku

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakanAWSPengelolaan Akun. Situs ini menunjukkan kepada Anda cara mengonfigurasi Pengelolaan Akun untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan lainnyaAWSlayanan yang membantu Anda memantau dan mengamankan sumber daya Pengelolaan Akun Anda.

Topik

- Perlindungan data dalam Manajemen AWS Akun
- AWS PrivateLinkuntukAWSPengelolaan Akun
- Identity and Access Management untuk Manajemen AWS Akun
- AWSkebijakan terkelola untukAWSManajemen Akun
- Validasi kepatuhan untuk Manajemen AWS Akun
- Ketahanan diAWSPengelolaan Akun
- Keamanan infrastruktur dalam AWS Account Management

Perlindungan data dalam Manajemen AWS Akun

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data dalam Manajemen AWS Akun. Sebagaimana diuraikan dalam model ini, AWS bertanggung jawab untuk memberikan perlindungan terhadap infrastruktur global yang menjalankan semua AWS Cloud. Anda harus bertanggung jawab untuk memelihara kendali terhadap konten yang di-hosting pada infrastruktur ini. Anda juga bertanggung jawab atas konfigurasi keamanan dan tugas manajemen untuk Layanan AWS yang Anda gunakan. Untuk informasi lebih lanjut tentang privasi data, lihat FAQ tentang Privasi Data. Untuk informasi tentang perlindungan data di Eropa, lihat postingan blog Model Tanggung Jawab Bersama AWS dan GDPR di Blog Keamanan AWS.

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara tersebut, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tugas pekerjaan mereka. Kami juga merekomendasikan agar Anda mengamankan data Anda dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk melakukan komunikasi dengan sumber daya AWS. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan log aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnyaLayanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi lebih lanjut tentang titik akhir FIPS yang tersedia, lihat Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi rahasia atau sensitif, seperti alamat email pelanggan Anda, ke dalam tag atau bidang teks bentuk bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Manajemen Akun atau lainnya Layanan AWS menggunakan konsol, APIAWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tag atau bidang teks bentuk bebas yang digunakan untuk nama dapat digunakan untuk penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, sebaiknya Anda

tidak menyertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

AWS PrivateLinkuntukAWSPengelolaan Akun

Jika Anda menggunakan Amazon Virtual Private Cloud (Amazon VPC) untuk meng-host AndaAWSsumber daya, Anda dapat mengaksesAWSLayanan Manajemen Akun dari dalam VPC tanpa harus melewati internet publik.

Amazon VPC memungkinkan Anda meluncurkan sumber daya AWS dalam jaringan virtual kustom. Anda dapat menggunakan VPC untuk mengendalikan pengaturan jaringan, seperti rentang alamat IP, subnet, tabel rute, dan gateway jaringan. Untuk informasi lebih lanjut tentang Amazon VPC, lihat Panduan Pengguna Amazon VPC.

Untuk menghubungkan Amazon VPC ke Manajemen Akun, Anda harus terlebih dahulu menentukanVPC antarmuka, yang memungkinkan Anda menghubungkan VPC Anda ke yang lainAWSlayanan. Titik akhir memberikan konektivitas yang dapat andal, dapat diskalakan, tanpa memerlukan gateway internet, instans terjemahan alamat jaringan (NAT), atau koneksi VPN. Untuk informasi selengkapnya, lihat VPC Endpoint Antarmuka (AWS PrivateLink) dalam Panduan Pengguna Amazon VPC.

Membuat Titik Akhir

Anda dapat membuatAWSTitik akhir Manajemen Akun di VPC Anda menggunakanAWS Management Console, yangAWS Command Line Interface(AWS CLI), sebuahAWSSDK,AWSAPI Manajemen Akun, atauAWS CloudFormation.

Untuk informasi tentang membuat dan mengonfigurasi titik akhir menggunakan konsol Amazon VPC atau AWS CLI, lihat Membuat Titik Akhir Antarmuka dalam Panduan Pengguna Amazon VPC.

> **Note**
>
> Ketika Anda membuat titik akhir, tetapkan Pengelolaan Akun sebagai layanan yang ingin Anda hubungkan ke VPC Anda, menggunakan format berikut:
>
> ```
> com.amazonaws.us-east-1.account
> ```

Anda harus menggunakan string persis seperti yang ditunjukkan, menentukan`us-east-1`Wilayah. Sebagai layanan global, Manajemen Akun di-host hanya dalam satuAWSWilayah.

Untuk informasi tentang membuat dan mengonfigurasi titik akhir menggunakan AWS CloudFormation, lihat sumber daya AWS::EC2::VPCEndpoint di AWS CloudFormationPanduan Pengguna.

Kebijakan Amazon VPC Endpoint

Anda dapat mengontrol tindakan apa yang dapat dilakukan melalui titik akhir layanan ini dengan melampirkan kebijakan endpoint saat Anda membuat titik akhir Amazon VPC. Anda dapat membuat aturan IAM kompleks dengan melampirkan beberapa kebijakan titik akhir. Untuk informasi selengkapnya, lihat :

- Kebijakan Amazon Virtual Private Cloud untuk Pengelolaan Akun
- Mengontrol Akses ke Layanan dengan VPC EndpointsdiAWS PrivateLinkPanduan.

Kebijakan Amazon Virtual Private Cloud untuk Pengelolaan Akun

Anda dapat membuat kebijakan Amazon VPC endpoint untuk Pengelolaan Akun yang di dalamnya Anda menentukan hal-hal berikut:

- Principal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan oleh prinsip.
- Sumber daya untuk melakukan tindakan.

Contoh berikut menunjukkan kebijakan Amazon VPC endpoint yang memungkinkan satu pengguna IAM bernama Alice di akun 123456789012 untuk mengambil dan mengubah informasi kontak alternatif untuk semuaAkun AWS, tetapi menolak semua pengguna IAM izin untuk menghapus informasi kontak alternatif pada akun apa pun.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Action": [
                "account:GetAlternateContact",
                "account:PutAlternateContact"
            ],
            "Resource": "arn:aws::iam:*:account,
            "Effect": "Allow",
            "Principal": {
              "AWS": "arn:aws::iam:123456789012:user/Alice"
            }
        },
        {
            "Action": "account:DeleteAlternateContact",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "arn:aws::iam:*:root"
        }
    ]
}
```

Jika Anda ingin memberikan akses ke akun yang merupakan bagian dariAWSOrganisasi ke kepala sekolah yang ada di salah satu akun anggota organisasi, maka`Resource`elemen harus menggunakan format berikut:

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

Untuk informasi selengkapnya tentang membuat kebijakan titik akhir, lihatMengontrol Akses ke Layanan dengan VPC EndpointsdiAWS PrivateLinkPanduan.

Identity and Access Management untuk Manajemen AWS Akun

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke sumber daya AWS secara aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Manajemen Akun. IAM adalah layanan Layanan AWS yang dapat Anda gunakan tanpa dikenakan biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan

- Bagaimana Manajemen AWS Akun bekerja dengan IAM
- Contoh kebijakan berbasis identitas untuk Manajemen Akun AWS
- Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk Manajemen Akun AWS
- Memecahkan masalah identitas dan akses Manajemen AWS Akun

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Manajemen Akun.

Pengguna layanan — Jika Anda menggunakan layanan Manajemen Akun untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Manajemen Akun untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Manajemen Akun, lihatMemecahkan masalah identitas dan akses Manajemen AWS Akun.

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Manajemen Akun di perusahaan Anda, Anda mungkin memiliki akses penuh ke Manajemen Akun. Tugas Anda adalah menentukan fitur dan sumber daya Manajemen Akun mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Manajemen Akun, lihatBagaimana Manajemen AWS Akun bekerja dengan IAM.

Administrator IAM — Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Manajemen Akun. Untuk melihat contoh kebijakan berbasis identitas Manajemen Akun yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk Manajemen Akun AWS

Mengautentikasi dengan identitas

Autentikasi adalah cara Anda untuk masuk ke AWS menggunakan kredensial identitas Anda. Anda harus terautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk ke AWS sebagai identitas terfederasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. Pengguna AWS IAM Identity Center Pengguna (Pusat Identitas

IAM), autentikasi Single Sign-On perusahaan Anda, dan kredensial Google atau Facebook Anda merupakan contoh identitas terfederasi. Saat Anda masuk sebagai identitas gabungan, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil suatu peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal akses AWS. Untuk informasi selengkapnya tentang cara masuk ke AWS, lihat Cara masuk ke Akun AWS dalam Panduan Pengguna AWS Sign-In.

Jika Anda mengakses AWS secara terprogram, AWS memberikan Kit Pengembangan Perangkat Lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensial Anda. Jika Anda tidak menggunakan peralatan AWS, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang cara menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan API AWS dalam Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Sebagai contoh, AWS menyarankan Anda menggunakan autentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) di AWS dalam Panduan Pengguna IAM.

Pengguna root Akun AWS

Ketika membuat Akun AWS, Anda memulai dengan satu identitas masuk yang memiliki akses penuh ke semua Layanan AWS dan sumber daya di akun tersebut. Identitas ini disebut pengguna root Akun AWS dan diakses dengan cara masuk menggunakan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari Anda. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar tugas lengkap yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas terfederasi

Praktik terbaiknya adalah mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensial temporer.

Identitas terfederasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, AWS Directory Service, direktori Pusat Identitas, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensial yang disediakan melalui sumber identitas. Ketika identitas terfederasi mengakses Akun AWS, identitas tersebut mengambil peran, dan peran ini memberikan kredensial sementara.

Untuk pengelolaan akses terpusat, sebaiknya Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apa yang dimaksud Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center.

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam Akun AWS Anda yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya andalkan kredensial temporer, dan bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan pengguna IAM, sebaiknya rotasikan kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan kumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk sekelompok besar pengguna. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran tersebut dimaksudkan untuk dapat diambil oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, silakan lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM merupakan identitas dalam Akun AWS Anda yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara dalam AWS Management Console dengan berganti peran. Anda dapat mengambil

peran dengan cara memanggil operasi API AWS CLI atau AWS atau menggunakan URL kustom. Untuk informasi selengkapnya tentang metode untuk menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas gabungan, Anda dapat membuat peran dan menentukan izin untuk peran tersebut. Saat identitas terfederasi diautentikasi, identitas tersebut dikaitkan dengan peran dan diberikan izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda mengonfigurasi sekumpulan izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengaitkan izin yang ditetapkan ke peran dalam IAM. Untuk informasi tentang rangkaian izin, lihat Rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center.
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) dengan akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, pada beberapa Layanan AWS, Anda dapat menyertakan kebijakan secara langsung ke sumber daya (bukan menggunakan peran sebagai proksi). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.
- Akses lintas layanan – Sebagian Layanan AWS menggunakan fitur di Layanan AWS lainnya. Contoh, ketika Anda melakukan panggilan dalam layanan, umumnya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Suatu layanan mungkin melakukan hal tersebut menggunakan izin pengguna utama panggilan, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses maju (FAS) – Ketika Anda menggunakan pengguna IAM atau peran IAM untuk melakukan tindakan di AWS, Anda akan dianggap sebagai seorang pengguna utama. Saat menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian dilanjutkan oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya diajukan saat layanan menerima permintaan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya

lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Meneruskan sesi akses.

- Peran IAM – Peran layanan adalah peran IAM yang diambil layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
- Peran terkait layanan – Peran terkait layanan adalah tipe peran layanan yang terkait dengan Layanan AWS. Layanan tersebut dapat mengambil peran untuk melakukan sebuah tindakan atas nama Anda. Peran terkait layanan akan muncul di Akun AWS Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

- Aplikasi yang berjalan di Amazon EC2 – Anda dapat menggunakan peran IAM untuk mengelola kredensial sementara untuk aplikasi yang berjalan di instans EC2 dan mengajukan permintaan API AWS CLI atau AWS. Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan peran AWS ke instans EC2 dan menyediakannya bagi semua aplikasinya, Anda dapat membuat profil instans yang dilampirkan ke instans tersebut. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengendalikan akses di AWS dengan membuat kebijakan dan melampirkannya ke identitas atau sumber daya AWS. Kebijakan adalah objek di AWS yang, ketika terkait dengan identitas atau sumber daya, akan menentukan izinnya. AWS mengevaluasi kebijakan-kebijakan tersebut ketika seorang pengguna utama (pengguna, pengguna root, atau sesi peran) mengajukan permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan di AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, silakan lihat Gambaran Umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses terhadap apa. Artinya, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat menjalankan peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk operasi. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut dapat memperoleh informasi peran dari AWS Management Console, AWS CLI, atau API AWS.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan pengguna dan peran, di sumber daya mana, dan dengan ketentuan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan terkelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran di Akun AWS Anda. Kebijakan terkelola meliputi kebijakan yang dikelola AWS dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan inline, lihat Memilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya yang dilampiri kebijakan tersebut, kebijakan ini menentukan jenis tindakan yang dapat dilakukan oleh pengguna utama tertentu di sumber daya tersebut dan apa ketentuannya. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan yang dikelola AWS dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, silakan lihat Gambaran umum daftar kontrol akses (ACL) di Panduan Developer Layanan Penyimpanan Ringkas Amazon.

Tipe kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Tipe-tipe kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda berdasarkan tipe kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan di mana Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan secara eksplisit terhadap salah satu kebijakan ini akan mengesampingkan izin tersebut. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – SCP adalah kebijakan JSON yang menentukan izin maksimum untuk sebuah organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola beberapa akun Akun AWS yang dimiliki bisnis Anda secara terpusat. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas dalam akun anggota, termasuk setiap Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda teruskan sebagai parameter saat Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran

dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit di salah satu kebijakan ini akan membatalkan izin tersebut. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Jika beberapa jenis kebijakan diberlakukan untuk satu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan ketika ada beberapa jenis kebijakan, lihat Logika evaluasi kebijakan dalam Panduan Pengguna IAM.

Bagaimana Manajemen AWS Akun bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Manajemen Akun, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Manajemen Akun.

Fitur IAM yang dapat Anda gunakan dengan Manajemen AWS Akun

Fitur IAM	Dukungan Manajemen Akun
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci persyaratan kebijakan	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Izin pengguna utama	Ya
Peran layanan	Tidak
Peran terkait layanan	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Manajemen Akun dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat AWSlayanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Manajemen Akun

Mendukung kebijakan berbasis identitas	Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan pengguna dan peran, di sumber daya mana, dan dengan ketentuan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak, serta ketentuan terkait jenis tindakan yang diizinkan atau ditolak. Anda tidak dapat menentukan pengguna utama dalam kebijakan berbasis identitas karena kebijakan ini berlaku untuk pengguna atau peran yang dilampiri kebijakan. Untuk mempelajari semua elemen yang dapat digunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Manajemen Akun

Untuk melihat contoh kebijakan berbasis identitas Manajemen Akun, lihat. Contoh kebijakan berbasis identitas untuk Manajemen Akun AWS

Kebijakan berbasis sumber daya dalam Manajemen Akun

Mendukung kebijakan berbasis sumber daya	Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya yang dilampiri kebijakan tersebut, kebijakan ini menentukan jenis tindakan yang

dapat dilakukan oleh pengguna utama tertentu di sumber daya tersebut dan apa ketentuannya. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau entitas IAM di akun lain sebagai pengguna utama dalam kebijakan berbasis sumber daya. Menambahkan pengguna utama lintas akun ke kebijakan berbasis sumber daya bagian dari membangun hubungan kepercayaan. Ketika pengguna utama dan sumber daya berada di Akun AWS yang berbeda, administrator IAM di akun tepercaya juga harus memberikan izin kepada entitas pengguna utama (pengguna atau peran) untuk mengakses sumber daya. Izin diberikan dengan melampirkan kebijakan berbasis identitas ke entitas tersebut. Namun, jika kebijakan berbasis sumber daya memberikan akses kepada pengguna utama dalam akun yang sama, kebijakan berbasis identitas lainnya tidak diperlukan. Untuk informasi selengkapnya, lihat Perbedaan peran IAM dengan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Tindakan kebijakan untuk Manajemen Akun

Mendukung tindakan kebijakan	Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan siapa yang memiliki akses ke apa. Yaitu, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama seperti operasi API AWS terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam suatu kebijakan untuk memberikan izin melakukan operasi terkait.

Untuk melihat daftar tindakan Manajemen Akun, lihat Tindakan yang ditentukan oleh Manajemen AWS Akun di Referensi Otorisasi Layanan.

Tindakan kebijakan dalam Manajemen Akun menggunakan awalan berikut sebelum tindakan.

```
account
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan-tindakan tersebut dengan koma.

```
"Action": [
      "account:action1",
      "account:action2"
         ]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Misalnya, untuk menentukan semua tindakan yang bekerja dengan kontak alternatif Akun AWS seseorang, sertakan tindakan berikut.

```
"Action": "account:*AlternateContact"
```

Untuk melihat contoh kebijakan berbasis identitas Manajemen Akun, lihat. Contoh kebijakan berbasis identitas untuk Manajemen Akun AWS

Sumber daya kebijakan untuk Manajemen Akun

Mendukung sumber daya kebijakan	Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan siapa yang memiliki akses ke apa. Yaitu, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek atau beberapa objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk mengindikasikan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Layanan Manajemen Akun mendukung jenis sumber daya spesifik berikut dalam `Resources` elemen kebijakan IAM untuk membantu Anda memfilter kebijakan dan membedakan antara jenis Akun AWS berikut:

- akun

  `resource`Jenis ini hanya cocok dengan akun mandiri Akun AWS yang bukan akun anggota dalam organisasi yang dikelola oleh AWS Organizations layanan.
- accountInOrganization

  `resource`Jenis ini hanya Akun AWS cocok dengan akun anggota dalam organisasi yang dikelola oleh AWS Organizations layanan.

Untuk melihat daftar jenis sumber daya Manajemen Akun dan ARNnya, lihat Sumber daya yang ditentukan oleh Manajemen AWS Akun di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh Manajemen AWS Akun.

Untuk melihat contoh kebijakan berbasis identitas Manajemen Akun, lihat. Contoh kebijakan berbasis identitas untuk Manajemen Akun AWS

Kunci kondisi kebijakan untuk Manajemen Akun

Mendukung kunci kondisi kebijakan spesifik layanan	Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan siapa yang memiliki akses ke apa. Yaitu, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) memungkinkan Anda menentukan kondisi di mana suatu pernyataan akan diterapkan. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi kondisional yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam satu pernyataan, atau beberapa kunci dalam satu elemen `Condition`, AWS akan mengevaluasinya dengan menggunakan operasi `AND`

logis. Jika Anda menentukan beberapa niilai untuk satu kunci persyaratan, AWS akan mengevaluasi syarat tersebut menggunakan operasi OR yang logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, silakan lihat Elemen kebijakan IAM: variabel dan tanda di Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi spesifik layanan. Untuk melihat semua kunci kondisi global AWS, lihat kunci konteks kondisi global AWS dalam Panduan Pengguna IAM.

Layanan Manajemen Akun mendukung kunci kondisi berikut yang dapat Anda gunakan untuk memberikan pemfilteran halus untuk kebijakan IAM Anda:

- akun: TargetRegion

  Kunci kondisi ini mengambil argumen yang terdiri dari daftar kode AWS Wilayah. Ini memungkinkan Anda memfilter kebijakan agar hanya memengaruhi tindakan yang berlaku pada Wilayah yang ditentukan.
- akun: AlternateContactTypes

  Kunci kondisi ini mengambil daftar jenis kontak alternatif:
  - PENAGIHAN
  - OPERASI
  - SEKURITI

  Menggunakan kunci ini memungkinkan Anda memfilter permintaan hanya untuk tindakan yang menargetkan jenis kontak alternatif yang ditentukan.
- akun: AccountResourceOrgPaths

  Kunci kondisi ini mengambil argumen yang terdiri dari daftar ARN dengan wildcard yang mewakili akun dalam organisasi. Ini memungkinkan Anda memfilter kebijakan agar hanya memengaruhi tindakan yang menargetkan akun dengan ARN yang cocok. Misalnya, ARN berikut hanya cocok dengan akun tersebut di organisasi yang ditentukan dan unit organisasi yang ditentukan (OU).

  ```
  arn:aws:account::111111111111:ou/o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
  ```
- akun: AccountResourceOrgTags

Kunci kondisi ini mengambil argumen yang terdiri dari daftar kunci tag dan nilai. Ini memungkinkan Anda memfilter kebijakan untuk hanya memengaruhi akun yang merupakan anggota organisasi dan yang ditandai dengan kunci dan nilai tag yang ditentukan.

Untuk melihat daftar kunci kondisi Manajemen Akun, lihat Kunci kondisi untuk Manajemen AWS Akun di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Manajemen AWS Akun.

Untuk melihat contoh kebijakan berbasis identitas Manajemen Akun, lihat. Contoh kebijakan berbasis identitas untuk Manajemen Akun AWS

Daftar kontrol akses di Manajemen Akun

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengontrol pengguna utama (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL sama dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

Kontrol akses berbasis atribut dengan Manajemen Akun

Mendukung ABAC (tanda dalam kebijakan)	Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Di AWS, atribut ini disebut tag. Anda dapat melampirkan tanda ke entitas IAM (pengguna atau peran) dan ke banyak sumber daya AWS. Pemberian tanda ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi-operasi ketika tanda milik pengguna utama cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna dalam situasi di mana pengelolaan kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tanda di elemen syarat dari sebuh kebijakan dengan menggunakan kunci-kunci persyaratan `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi hanya untuk beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? di Panduan Pengguna IAM. Untuk melihat tutorial terkait langkah-langkah penyiapan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di Panduan Pengguna IAM.

Menggunakan kredensi sementara dengan Manajemen Akun

Mendukung kredensial sementara	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensial sementara. Sebagai informasi tambahan, termasuk tentang Layanan AWS mana saja yang berfungsi dengan kredensial sementara, lihat Layanan AWS yang berfungsi dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensial sementara jika Anda masuk ke AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS dengan menggunakan tautan masuk tunggal (SSO) milik perusahaan Anda, proses itu secara otomatis akan membuat kredensial temporer. Anda juga akan membuat kredensial sementara secara otomatis saat masuk ke konsol sebagai pengguna dan kemudian beralih peran. Untuk informasi selengkapnya tentang cara beralih peran, lihat Beralih peran (konsol) di Panduan Pengguna IAM.

Anda dapat membuat kredensial sementara secara manual menggunakan AWS CLI atau AWS API. Anda kemudian dapat menggunakan kredensial sementara untuk mengakses AWS. AWS menyarankan Anda membuat kredensial sementara secara dinamis, alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Izin utama lintas layanan untuk Manajemen Akun

Mendukung sesi akses maju (FAS)	Ya

Jika menggunakan pengguna IAM atau peran IAM untuk melakukan tindakan di AWS, Anda akan dianggap sebagai pengguna utama. Jika menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian dilanjutkan oleh tindakan lain di layanan yang berbeda. FAS menggunakan

izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya diajukan saat layanan menerima permintaan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Meneruskan sesi akses.

Peran layanan untuk Manajemen Akun

Mendukung peran layanan	Tidak

Peran layanan adalah sebuah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

Peran terkait layanan untuk Manajemen Akun

Mendukung peran terkait layanan	Tidak

Peran tertaut layanan adalah jenis peran layanan yang terkait dengan Layanan AWS. Layanan ini dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan akan muncul di Akun AWS Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau pengelolaan peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Temukan sebuah layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Manajemen Akun AWS

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau mengubah sumber daya Manajemen Akun. Pengguan dan peran tersebut juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau API

AWS. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat menjalankan peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Manajemen Akun, termasuk format ARN untuk setiap jenis sumber daya, lihat Tindakan, sumber daya, dan kunci kondisi untuk Manajemen AWS Akun dalam Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan halaman Akun di AWS Management Console
- Menyediakan akses hanya-baca ke halaman Akun di AWS Management Console
- Memberikan akses penuh ke halaman Akun di AWS Management Console

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Manajemen Akun di akun Anda. Tindakan ini dikenai biaya untuk Akun AWS Anda. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulai menggunakan kebijakan yang dikelola AWS dan beralih ke izin dengan hak akses paling rendah – Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan yang dikelola AWS yang memberikan izin untuk banyak kasus penggunaan umum. Kebijakan ini ada di Akun AWS Anda. Sebaiknya Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan AWS yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan yang dikelola AWS atau kebijakan yang dikelola AWS untuk fungsi pekerjaan di Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk menerapkan izin, lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.

- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis syarat kebijakan untuk menentukan bahwa semua pengajuan harus dikirim menggunakan SSL. Anda juga dapat menggunakan kondisi untuk memberi akses ke tindakan layanan jika digunakan melalui Layanan AWS yang spesifk, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.
- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat validasi kebijakan Analizer Akses IAM di Panduan Pengguna IAM.
- Wajibkan autentikasi multi-faktor (MFA) – Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Akun AWS Anda, aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM di Panduan Pengguna IAM.

Menggunakan halaman Akun di AWS Management Console

Untuk mengakses halaman Akun diAWS Management Console, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang AndaAkun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tersebut tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna IAM atau peran) dengan kebijakan tersebut.

Untuk memastikan bahwa pengguna dan peran dapat menggunakan konsol Manajemen Akun, Anda dapat memilih untuk melampirkan kebijakan `AWSAccountManagementReadOnlyAccess` atau `AWSAccountManagementFullAccess` AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna di Panduan Pengguna IAM.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, dalam banyak kasus, Anda dapat memilih

untuk mengizinkan akses hanya ke tindakan yang cocok dengan operasi API yang Anda coba lakukan.

Menyediakan akses hanya-baca ke halaman Akun di AWS Management Console

Dalam contoh berikut, Anda ingin memberikan pengguna IAM di akses Akun AWS hanya-baca ke halaman Akun di halaman. AWS Management Console Pengguna dengan kebijakan ini terlampir tidak dapat melakukan perubahan apa pun.

`account:GetAccountInformation`Tindakan memberikan akses untuk melihat sebagian besar pengaturan di halaman Akun. Namun, untuk melihat AWS Wilayah yang saat ini diaktifkan, Anda juga harus menyertakan `account:ListRegions` tindakan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantReadOnlyAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Memberikan akses penuh ke halaman Akun di AWS Management Console

Dalam contoh berikut, Anda ingin memberikan pengguna IAM dalam akses Akun AWS penuh Anda ke halaman Akun di AWS Management Console halaman. Pengguna dengan kebijakan ini terlampir dapat mengubah pengaturan untuk akun.

Kebijakan contoh ini dibuat berdasarkan kebijakan contoh sebelumnya dengan menambahkan setiap izin tulis yang tersedia (kecuali CloseAccount), yang memungkinkan pengguna mengubah sebagian besar pengaturan untuk akun, termasuk izin dan izin. `account:EnableRegion` `account:DisableRegion`

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantFullAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions",
                "account:PutContactInformation",
                "account:PutChallengeQuestions",
                "account:PutAlternateContact",
                "account:DeleteAlternateContact",
                "account:EnableRegion",
                "account:DisableRegion"
            ],
            "Resource": "*"
        }
    ]
}
```

Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk Manajemen Akun AWS

Untuk diskusi lengkap tentang akun AWS dan pengguna IAM, lihat Apa itu IAM? di Panduan Pengguna IAM.

Untuk petunjuk tentang cara memperbarui kebijakan terkelola pelanggan, lihat Mengedit kebijakan terkelola pelanggan (konsol) di Panduan Pengguna IAM.

AWSKebijakan tindakan Manajemen Akun

Tabel ini merangkum izin yang memberikan akses ke pengaturan akun Anda. Untuk contoh kebijakan yang menggunakan izin ini, lihat contoh kebijakan Manajemen AWS Akun.

> **Note**
>
> Untuk memberikan akses tulis kepada pengguna IAM ke setelan akun tertentu di halaman AkunAWS Management Console, Anda harus mengizinkan `GetAccountInformation` izin, selain izin (atau izin) yang ingin Anda gunakan untuk mengubah setelan itu.

Nama izin	Tingkat akses	Deskripsi
`account:ListRegions`	Daftar	Memberikan izin untuk membuat daftar Wilayah yang tersedia.
`account:GetAccount Information`	Baca	Memberikan izin untuk mengambil informasi akun untuk akun.
`account:GetAlterna teContact`	Baca	Memberikan izin untuk mengambil kontak alternatif untuk akun.
`account:GetChallen geQuestions`	Baca	Memberikan izin untuk mengambil pertanyaan tantangan untuk akun.
`account:GetContact Information`	Baca	Memberikan izin untuk mengambil informasi kontak utama untuk akun.
`account:GetRegionO ptStatus`	Baca	Memberikan izin untuk mendapatkan status keikutser taan suatu Wilayah.
`account:CloseAccount`	Tulis	Memberikan izin untuk menutup akun. **Note** Ini adalah izin untuk konsol saja. Tidak ada akses API yang tersedia untuk izin ini.

Nama izin	Tingkat akses	Deskripsi
`account:DeleteAlternateContact`	Tulis	Memberikan izin untuk menghapus kontak alternatif untuk akun.
`account:DisableRegion`	Tulis	Memberikan izin untuk menonaktifkan penggunaan Wilayah.
`account:EnableRegion`	Tulis	Memberikan izin untuk mengaktifkan penggunaan Wilayah.
`account:PutAlternateContact`	Tulis	Memberikan izin untuk memodifikasi kontak alternatif untuk akun.
`account:PutChallengeQuestions`	Tulis	Memberikan izin untuk memodifikasi pertanyaan tantangan untuk akun. **Note** Ini adalah izin untuk konsol saja. Tidak ada akses API yang tersedia untuk izin ini.
`account:PutContactInformation`	Tulis	Memberikan izin untuk memperbarui informasi kontak utama untuk akun.

Memecahkan masalah identitas dan akses Manajemen AWS Akun

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Manajemen Akun dan IAM.

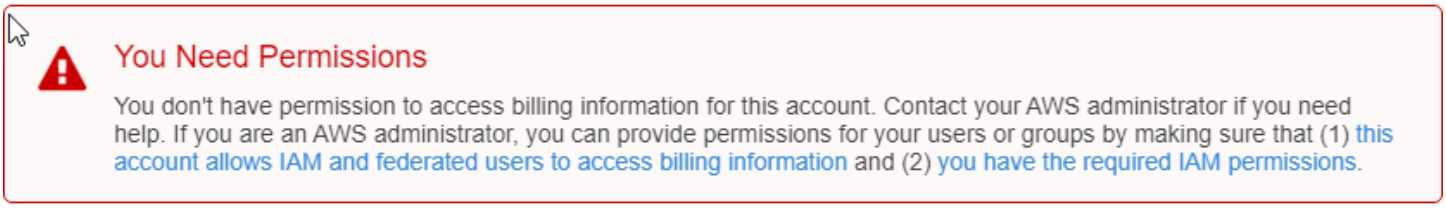
Topik

- Saya tidak berwenang untuk melakukan tindakan di halaman Akun
- Saya tidak berwenang untuk melakukan iam:PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses detail akun saya

Saya tidak berwenang untuk melakukan tindakan di halaman Akun

Jika AWS Management Console memberi tahu bahwa Anda tidak diotorisasi untuk melakukan tindakan, Anda harus menghubungi administrator untuk mendapatkan bantuan. Administrator adalah orang yang memberikan nama pengguna dan kata sandi kepada Anda.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` IAM mencoba menggunakan konsol untuk melihat detail tentang miliknya Akun AWS di halaman Akun AWS Management Console tetapi tidak memiliki `account:GetAccountInformation` izin.



Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk mengizinkan dia mengakses sumber daya *`my-example-widget`* menggunakan tindakan `account:`*`GetWidget`*.

Saya tidak berwenang untuk melakukan **`iam:PassRole`**

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Manajemen Akun.

Sebagian Layanan AWS mengizinkan Anda untuk memberikan peran yang sudah ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait-layanan. Untuk melakukan tindakan tersebut, Anda harus memiliki izin untuk memberikan peran pada layanan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan dalam Manajemen Akun. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda membutuhkan bantuan, hubungi administrator AWS Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses detail akun saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau pengguna di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi pengguna akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mengetahui apakah Manajemen Akun mendukung fitur ini, lihatBagaimana Manajemen AWS Akun bekerja dengan IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya di seluruh Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di Akun AWS lainnya yang Anda miliki dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya Anda ke pihak ketiga Akun AWS, lihat Menyediakan akses ke akun Akun AWS yang dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (gabungan identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan antara peran IAM dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

AWSkebijakan terkelola untukAWSManajemen Akun

AWSManajemen Akun saat ini menyediakan duaAWSkebijakan terkelola yang tersedia untuk Anda gunakan:

- Kebijakan terkelola AWS: AWSAccountManagementReadOnlyAccess

- Kebijakan terkelola AWS: AWSAccountManagementFullAccess
- Pembaruan Manajemen Akun keAWSkebijakan terkelola

SebuahAWSkebijakan terkelola adalah kebijakan mandiri yang dibuat dan dikelola olehAWS.AWSkebijakan terkelola dirancang untuk memberikan izin untuk banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwaAWSkebijakan terkelola mungkin tidak memberikan izin hak istimewa untuk kasus penggunaan spesifik Anda karena tersedia untuk semuaAWSpelanggan untuk digunakan. Kami menyarankan Anda mengurangi izin lebih lanjut dengan mendefinisikankebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalamAWSkebijakan yang dikelola. JikaAWSupdate izin didefinisikan dalamAWSkebijakan terkelola, pembaruan mempengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan.AWSkemungkinan besar akan memperbaruiAWSkebijakan terkelola saat baruLayanan AWSdiluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

Kebijakan terkelola AWS: AWSAccountManagementReadOnlyAccess

Anda dapat melampirkan kebijakan `AWSAccountManagementReadOnlyAccess` ke identitas-identitas IAM Anda.

Kebijakan ini menyediakan izin hanya-baca untuk hanya melihat hal berikut:

- Metadata tentangAkun AWS
- YangWilayah AWSyang diaktifkan atau dinonaktifkan untukAkun AWS(Anda dapat melihat status Wilayah di akun Anda hanya dengan menggunakanAWSkonsol)

Hal ini dilakukan dengan memberikan izin untuk menjalankan salah satu`Get*`atau`List*`operasi. Ini tidak memberikan kemampuan apa pun untuk memodifikasi metadata akun atau mengaktifkan atau menonaktifkanWilayah AWSuntuk akun.

Detail izin

Kebijakan ini mencakup izin berikut.

- `account`- Memungkinkan prinsipal untuk mengambil informasi metadata tentangAkun AWS. Hal ini juga memungkinkan prinsipal untuk daftarWilayah AWSyang diaktifkan untuk akun diAWS Management Console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "account:Get*",
                "account:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Kebijakan terkelola AWS: AWSAccountManagementFullAccess

Anda dapat melampirkan kebijakan `AWSAccountManagementFullAccess` ke identitas-identitas IAM Anda.

Kebijakan ini menyediakan akses administratif penuh untuk melihat atau memodifikasi hal-hal berikut:

- Metadata tentangAkun AWS
- YangWilayah AWSyang diaktifkan atau dinonaktifkan untukAkun AWS(Anda dapat melihat status atau mengaktifkan atau menonaktifkan Wilayah untuk akun Anda hanya dengan menggunakanAWSkonsol)

Hal ini dilakukan dengan memberikan izin untuk menjalankan apapun`account`operasi.

Detail izin

Kebijakan ini mencakup izin berikut.

- `account`- Memungkinkan prinsipal untuk melihat atau memodifikasi informasi metadata tentangAkun AWS. Hal ini juga memungkinkan prinsipal untuk daftarWilayah AWSyang diaktifkan untuk akun dan mengaktifkan atau menonaktifkannya diAWS Management Console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "account:*",
            "Resource": "*"
        }
    ]
}
```

Pembaruan Manajemen Akun keAWSkebijakan terkelola

Lihat detail tentang pembaruan keAWSkebijakan terkelola untuk Manajemen Akun sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat dokumen manajemen akun.

Perubahan	Deskripsi	Tanggal
AWSManajemen Akun diluncurkan dengan yang baruAWSkebijakan terkelola dan mulai melacak perubahan	Manajemen Akun awalnya diluncurkan dengan berikut iniAWSkebijakan terkelola: • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess	30 September 2021

Validasi kepatuhan untuk Manajemen AWS Akun

Auditor pihak ketiga menilai keamanan dan kepatuhan AWS layanan yang dapat dijalankan di Anda Akun AWS sebagai bagian dari beberapa program AWS kepatuhan. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat Layanan AWSdalam lingkup oleh program kepatuhan Layanan AWS . Untuk informasi umum, lihat Program Kepatuhan AWS.

Anda bisa mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan dalam AWS Artifact dalam Panduan AWS Artifact Pengguna.

Tanggung jawab kepatuhan Anda saat menggunakan layanan di Anda Akun AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta hukum dan peraturan yang berlaku. AWSmenyediakan sumber daya berikut untuk membantu dengan kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan - Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

  > **Note**
  >
  > Tidak semua Layanan AWS memenuhi syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- Sumber Daya Kepatuhan AWS – Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- Mengevaluasi Sumber Daya dengan Aturan di Panduan Developer AWS Config – Layanan AWS Config menilai seberapa baik konfigurasi sumber daya Anda dalam mematuhi praktik-praktik internal, pedoman industri, dan regulasi internal.
- AWS Security Hub – Layanan AWS ini menyediakan pandangan yang komprehensif tentang status keamanan Anda dalam AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri dan praktik terbaik untuk keamanan.
- AWS Audit Manager – Layanan AWS ini akan membantu Anda untuk terus-menerus mengaudit penggunaan AWS untuk menyederhanakan bagaimana Anda mengelola risiko dan kepatuhan terhadap regulasi dan standar industri.

Ketahanan diAWSPengelolaan Akun

ParameterAWSinfrastruktur global dibangun di sekitarWilayah AWSdan Availability Zone. Wilayah menyediakan beberapa Availability Zone yang terpisah dan terisolasi secara fisik, yang terhubung melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Availability Zone,

Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis mengalami failover antar zona tanpa gangguan. Availability Zone memiliki ketersediaan yang lebih baik, toleran terhadap kegagalan, dan dapat diukur skalanya jika dibandingkan dengan satu atau beberapa infrastruktur pusat data tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur Global AWS.

Keamanan infrastruktur dalam AWS Account Management

Sebagai layanan terkelola, AWS layanan Akun AWS yang berjalan di Anda dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk merancang AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja Pilar Keamanan yang AWS Diarsiteksikan dengan Baik.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses pengaturan akun melalui jaringan. Klien harus mendukung hal berikut:

- Transport Layer Security (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju sempurna (PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan principal IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Memantau Pengelolaan AWS Akun

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Manajemen AWS Akun dan AWS solusi Anda yang lain. AWSmenyediakan alat pemantauan berikut untuk menonton Manajemen Akun, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- AWS CloudTrailmenangkap (log) panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama Anda Akun AWS dan menulis file log ke bucket Amazon Simple Storage Service (Amazon S3) yang Anda tentukan. Ini memungkinkan Anda mengidentifikasi pengguna dan akun mana yang dipanggilAWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.
- Amazon EventBridge menambahkan otomatisasi tambahan ke AWS layanan Anda dengan merespons secara otomatis peristiwa sistem, seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Acara dari AWS layanan dikirimkan ke EventBridge dalam waktu dekat. Anda dapat menuliskan aturan sederhana untuk menunjukkan peristiwa mana yang sesuai kepentingan Anda, dan tindakan otomatis mana yang diambil ketika suatu peristiwa sesuai dengan suatu aturan. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.

LoggingAWSPanggilan API Manajemen Akun menggunakanAWS CloudTrail

ParameterAWSAPI Manajemen Akun terintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atauAWSlayanan yang memanggil operasi Manajemen Akun. CloudTrail merekam semua panggilan API Manajemen Akun sebagai peristiwa. Panggilan yang diambil mencakup semua panggilan ke operasi Manajemen Akun. Jika membuat jejak, Anda dapat mengaktifkan pengiriman peristiwa CloudTrail berkelanjutan ke bucket Amazon S3, termasuk peristiwa untuk pengoperasian Manajemen Akun. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru dalam konsol CloudTrail di Riwayat peristiwa. Menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang disebut operasi Manajemen Akun, alamat IP yang digunakan untuk membuat permintaan dan kapan, dan detail lainnya.

Untuk mempelajari selengkapnya tentang CloudTrail, lihat Panduan Pengguna AWS CloudTrail.

Informasi Manajemen Akun di CloudTrail

CloudTrail diaktifkan diAkun AWSsaat Anda membuat akun. Saat aktivitas terjadi dengan operasi Manajemen Akun, CloudTrail mencatat aktivitas tersebut di CloudTrail bersama lainnyaAWSperistiwa layanan diRiwayat peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di Akun AWS Anda. Untuk informasi lebih lanjut, lihat Melihat Peristiwa dengan Riwayat Peristiwa CloudTrail.

Untuk catatan berkelanjutan tentang peristiwa diAkun AWS, termasuk peristiwa untuk operasi Manajemen Akun, buat jejak. Jejak memungkinkan CloudTrail mengirim file log ke bucket Amazon S3. Secara bawaan, saat Anda membuat jejak diAWS Management Console, jejak berlaku untuk semuaWilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengonfigurasi lainnyaAWSlayanan untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan di log CloudTrail. Untuk informasi selengkapnya, lihat yang berikut:

- Gambaran umum untuk membuat jejak
- Layanan dan integrasi yang didukung CloudTrail
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima berkas log CloudTrail dari beberapa Wilayah
- Menerima berkas log CloudTrail dari beberapa akun

AWS CloudTraillog semua operasi API Manajemen Akun yang ditemukan diReferensi APIbagian dari panduan ini. Misalnya, panggilan ke operasi `CreateAccount`, `DeleteAlternateContact`, dan `PutAlternateContact` menghasilkan entri di berkas log CloudTrail.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Apakah permintaan tersebut dibuat dengan pengguna root atauAWS Identity and Access Management(IAM) kredensi pengguna
- Apakah permintaan tersebut dibuat dengan kredensi keamanan sementara atau tidak untuk peran IAM atau pengguna gabungan
- Jika permintaan tersebut dibuat oleh layanan AWS lainnya

Untuk informasi selengkapnya, lihat elemen userIdentity CloudTrail.

Memahami entri log Manajemen Akun

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang telah Anda tentukan. File log CloudTrail berisi satu atau beberapa entri log. Acara mewakili satu permintaan dari sumber apa pun dan mencakup informasi tentang operasi yang diminta, tanggal dan waktu operasi, parameter permintaan, dan sebagainya. File log CloudTrail bukan jejak tumpukan terurut dari panggilan API publik, sehingga berkas tersebut tidak muncul dalam urutan tertentu.

Contoh 1: Contoh berikut menunjukkan entri log CloudTrail untuk panggilan ke`GetAlternateContact`operasi untuk mengambil arus`OPERATIONS`kontak alternatif untuk akun. Nilai yang dikembalikan oleh operasi tidak termasuk dalam informasi yang dicatat.

Example Contoh 1


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T19:25:53Z"
      }
    }
  },
  "eventTime": "2021-04-30T19:26:15Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "GetAlternateContact",
  "awsRegion": "us-east-1",
```

```
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "SECURITY"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-111111111111",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-222222222222",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

Contoh 2: Contoh berikut menunjukkan entri log CloudTrail untuk panggilan kePutAlternateContactoperasi untuk menambahkanBILLINGkontak alternatif ke akun.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:08Z",
  "eventSource": "account.amazonaws.com",
```

```
  "eventName": "PutAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "name": "*Alejandro Rosalez*",
    "emailAddress": "alrosalez@example.com",
    "title": "CFO",
    "alternateContactType": "BILLING"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-333333333333",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-444444444444",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

Contoh 3: Contoh berikut menunjukkan entri log CloudTrail untuk panggilan ke`DeleteAlternateContact`operasi untuk menghapus arus`OPERATIONS`kontak alternatif.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
```

```
      }
    }
  },
  "eventTime": "2021-04-30T18:33:16Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "DeleteAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "OPERATIONS"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-555555555555",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-666666666666",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```


Memantau acara Manajemen Akun dengan EventBridge

Amazon EventBridge, sebelumnya disebut CloudWatch Events, membantu Anda memantau peristiwa yang spesifik untuk dan memulai tindakan target yang menggunakan lainnya. Layanan AWS Acara dari Layanan AWS dikirim ke EventBridge dalam waktu dekat.

Dengan menggunakan EventBridge, Anda dapat membuat aturan yang cocok dengan peristiwa yang masuk dan merutekkannya ke target untuk diproses.

Untuk informasi selengkapnya, lihat Memulai Amazon EventBridge di Panduan EventBridge Pengguna Amazon.

Acara Manajemen Akun

Contoh berikut menunjukkan peristiwa untuk Manajemen Akun. Acara diproduksi atas dasar upaya terbaik.

Hanya peristiwa yang khusus untuk mengaktifkan dan menonaktifkan Regions dan panggilan API via yang saat ini CloudTrail tersedia untuk Manajemen Akun.

Tipe peristiwa

- Acara untuk mengaktifkan dan menonaktifkan Wilayah

Acara untuk mengaktifkan dan menonaktifkan Wilayah

Saat Anda mengaktifkan atau menonaktifkan Wilayah di akun, baik dari Konsol maupun dari API, tugas asinkron akan dimulai. Permintaan awal akan dicatat sebagai CloudTrail peristiwa di akun target. Selain itu, sebuah EventBridge acara akan dikirim ke akun panggilan ketika proses aktifkan atau nonaktifkan telah dimulai, dan sekali lagi setelah proses tersebut selesai.

Contoh peristiwa berikut menunjukkan bagaimana permintaan akan dikirim yang menunjukkan bahwa `2020-09-30` di `ap-east-1` Wilayah adalah `ENABLED` untuk akun`123456789012`.

```
{
   "version":"0",
   "id":"11112222-3333-4444-5555-666677778888",
   "detail-type":"Region Opt-In Status Change",
   "source":"aws.account",
   "account":"123456789012",
   "time":"2020-09-30T06:51:08Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:account::123456789012:account"
   ],
   "detail":{
      "accountId":"123456789012",
      "regionName":"ap-east-1",
      "status":"ENABLED"
   }
}
```

Ada empat kemungkinan status yang cocok dengan status yang dikembalikan oleh API `GetRegionOptStatus` dan`ListRegions`:

- `ENABLED`— Wilayah telah berhasil diaktifkan untuk yang `accountId` ditunjukkan
- `ENABLING`— Wilayah sedang dalam proses diaktifkan untuk yang `accountId` ditunjukkan
- `DISABLED`- Wilayah telah berhasil dinonaktifkan untuk yang `accountId` ditunjukkan
- `DISABLING`— Wilayah sedang dalam proses dinonaktifkan untuk yang `accountId` ditunjukkan

Contoh pola peristiwa berikut, membuat aturan yang menangkap semua peristiwa Region.

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ]
}
```

Contoh pola peristiwa berikut, menciptakan aturan yang hanya menangkap `ENABLED` dan peristiwa `DISABLED` Wilayah.

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ],
   "detail":{
      "status":[
         "DISABLED",
         "ENABLED"
      ]
   }
}
```

Referensi API

Operasi API dalam Manajemen Akun (`account`) namespace memungkinkan Anda untuk memodifikasiAkun AWS.

SetiapAkun AWSmendukung metadata dengan informasi tentang akun, termasuk informasi tentang hingga tiga kontak alternatif yang terkait dengan akun. Ini adalah tambahan ke alamat email yang terkait denganpengguna rootdari akun. Anda hanya dapat menentukan satu dari masing-masing jenis kontak berikut yang terkait dengan akun.

- Kontak penagihan
- Kontak operasi
- Kontak keamanan

Secara default, operasi API yang dibahas dalam panduan ini berlaku langsung ke akun yang memanggil operasi. Yangidentitasdi akun yang memanggil operasi biasanya merupakan peran IAM atau pengguna IAM dan harus memiliki izin yang diterapkan oleh kebijakan IAM untuk memanggil operasi API. Atau, Anda dapat memanggil operasi API ini dari identitas diAWS Organizationsakun manajemen dan tentukan nomor ID akun untukAkun AWSyang merupakan anggota organisasi.

Versi API

Versi Referensi API Akun ini mendokumentasikan API Manajemen Akun versi 2021-02-01.

> **Note**
>
> Sebagai alternatif untuk menggunakan API secara langsung, Anda dapat menggunakan salah satuAWSSDK, yang terdiri dari pustaka dan kode contoh untuk berbagai bahasa dan platform pemrograman (Java, Ruby, .NET, iOS, Android, dan lainnya). SDK menyediakan cara mudah untuk membuat akses terprogramAWSOrganisasi. Misalnya, SDK menangani permintaan penandatanganan secara kriptografis, mengelola kesalahan, dan mencoba ulang permintaan secara otomatis. Untuk informasi selengkapnya tentang AWS SDK, termasuk cara mengunduh dan menginstalnya, lihat Alat untuk Amazon Web Services.

Kami menyarankan Anda menggunakanAWSSDK untuk melakukan panggilan API terprogram ke layanan Manajemen Akun. Namun, Anda juga dapat menggunakan Account Management Query

API untuk melakukan panggilan langsung ke layanan web Manajemen Akun. Untuk mempelajari lebih lanjut tentang API Kueri Manajemen Akun, lihatMemanggil API dengan membuat permintaan Kueri HTTPdalam Panduan Pengguna Manajemen Akun. Organisasi mendukung permintaan GET dan POST untuk semua tindakan. Artinya, API tidak mewajibkan Anda menggunakan GET untuk beberapa tindakan dan POST untuk yang lainnya. Namun, permintaan GET harus memenuhi ukuran batas dari sebuah URL. Oleh karena itu, untuk operasi yang membutuhkan ukuran lebih besar, gunakan permintaan POST.

Permintaan penandatanganan

Saat Anda mengirim permintaan HTTP keAWS, Anda harus menandatangani permintaan sehinggaAWSdapat mengidentifikasi siapa yang mengirimnya. Anda menandatangani permintaan denganAWSkunci akses, yang terdiri dari ID kunci akses dan kunci akses rahasia. Kami sangat menyarankan agar Anda tidak membuat kunci akses untuk akun root Anda. Siapa pun yang memiliki kunci akses untuk akun root Anda memiliki akses tak terbatas ke semua sumber daya di akun Anda. Sebagai gantinya, buat kunci akses untuk pengguna IAM yang memiliki hak administratif. Sebagai pilihan lain, gunakanAWSSecurity Token Service untuk menghasilkan kredensi keamanan sementara, dan menggunakan kredensil tersebut untuk menandatangani permintaan.

Untuk menandatangani permintaan, sebaiknya gunakan Signature Version 4. Jika Anda memiliki aplikasi yang sudah ada yang menggunakan Signature Version 2, Anda tidak perlu memperbaruinya untuk menggunakan Signature Version 4. Namun, beberapa operasi sekarang memerlukan Signature Version 4. Dokumentasi untuk operasi yang memerlukan versi 4 menunjukkan persyaratan ini. Untuk informasi lebih lanjut, lihatPenandatangananAWSPermintaan APIdi dalamPanduan Pengguna IAM.

Bila Anda menggunakanAWSAntarmuka Baris Perintah (AWSCLI) atau salah satuAWSSDK untuk membuat permintaanAWS, alat ini secara otomatis menandatangani permintaan untuk Anda dengan kunci akses yang Anda tentukan saat Anda mengkonfigurasi alat.

Dukungan dan umpan balik untuk Manajemen Akun

Kami menyambut umpan balik Anda. Kirim komentar Anda kefeedback-awsaccounts@amazon.comatau posting umpan balik dan pertanyaan Anda diForum dukungan Manajemen Akun. Untuk informasi lebih lanjut tentangAWSforum dukungan, lihatBantuan Forum.

Bagaimana contoh disajikan

JSON yang dikembalikan oleh Manajemen Akun sebagai respons terhadap permintaan Anda dikembalikan sebagai string panjang tunggal tanpa jeda baris atau spasi pemformatan. Kedua jeda baris dan spasi ditampilkan dalam contoh dalam panduan ini untuk meningkatkan keterbacaan.

Ketika contoh parameter input juga akan menghasilkan string panjang yang akan melampaui layar, kita memasukkan jeda baris untuk meningkatkan keterbacaan. Anda harus selalu mengirimkan masukan sebagai string teks JSON tunggal.

Merekam Permintaan API

Dukungan Manajemen AkunCloudTrail, layanan yang mencatatAWSPanggilan API untukAkun AWSdan mengirimkan file log ke bucket Amazon S3. Dengan menggunakan informasi yang dikumpulkan olehCloudTrail, Anda dapat menentukan permintaan mana yang berhasil dibuat untuk Manajemen Akun, siapa yang membuat permintaan, kapan dibuat, dan sebagainya. Untuk selengkapnya tentang Manajemen Akun dan dukungannyaCloudTrail, lihatLoggingAWSPanggilan API Manajemen Akun menggunakanAWS CloudTrail. Untuk mempelajari lebih lanjut tentangCloudTrail, termasuk cara menyalakannya dan menemukan file log Anda, lihatAWS CloudTrailPanduan Pengguna.

Tindakan

Tindakan berikut didukung:

- DeleteAlternateContact
- DisableRegion
- EnableRegion
- GetAlternateContact
- GetContactInformation
- GetRegionOptStatus
- ListRegions
- PutAlternateContact
- PutContactInformation

DeleteAlternateContact

Menghapus kontak alternatif yang ditentukan dari fileAkun AWS.

Untuk detail selengkapnya tentang cara menggunakan operasi kontak alternatif, lihat Mengakses atau memperbarui kontak alternatif.

> **Note**
>
> Sebelum Anda dapat memperbarui informasi kontak alternatif untuk informasi Akun AWS yang dikelola olehAWS Organizations, Anda harus terlebih dahulu mengaktifkan integrasi antara Manajemen AWS Akun dan Organizations. Untuk informasi selengkapnya, lihat Mengaktifkan akses tepercaya untuk Manajemen AWS Akun.

Minta Sintaks

```
POST /deleteAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun AWS akun yang ingin Anda akses atau modifikasi dengan operasi ini.

Jika Anda tidak menentukan parameter ini, itu default ke AWS akun identitas yang digunakan untuk memanggil operasi.

Untuk menggunakan parameter ini, pemanggil harus berupa identitas di akun manajemen organisasi atau akun administrator yang didelegasikan, dan ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan semua fitur, dan organisasi harus mengaktifkan akses tepercaya untuk layanan Manajemen Akun, dan secara opsional akun admin yang didelegasikan ditetapkan.

> **Note**
>
> Akun manajemen tidak dapat menentukan sendiri`AccountId`; itu harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, maka jangan tentukan parameter ini, dan panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau ubah.

Jenis: String

Pola: `^\d{12}$`

Wajib: Tidak

AlternateContactType

Menentukan mana dari kontak alternatif untuk menghapus.

Jenis: String

Nilai yang Valid: `BILLING | OPERATIONS | SECURITY`

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

Kode Status HTTP: 403

InternalServerException

Operasi gagal karena kesalahan internal keAWS. Coba operasi Anda lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Operasi gagal karena menentukan sumber daya yang tidak dapat ditemukan.

Kode Status HTTP: 404

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

Kode Status HTTP: 400

Contoh

Contoh 1

Contoh berikut menghapus kontak alternatif keamanan untuk akun yang kredensialnya digunakan untuk memanggil operasi.

Sampel Permintaan

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact
```

```
{ "AlternateContactType": "SECURITY" }
```

Contoh Respons

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Contoh 2

Contoh berikut menghapus kontak alternatif penagihan untuk akun anggota yang ditentukan dalam suatu organisasi. Anda harus menggunakan kredensi dari akun manajemen organisasi atau dari akun admin yang didelegasikan oleh layanan Manajemen Akun.

Sampel Permintaan

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{ "AccountId": "123456789012", "AlternateContactType": "BILLING" }
```

Contoh Respons

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWSAntarmuka Baris Perintah
- AWSSDK for .NET
- AWSSDK for C++
- AWSSDK for Go
- AWSSDK for Java V2
- AWSSDK untuk V3 JavaScript
- AWSSDK for PHP V3

- AWSSDK untuk Python
- AWSSDK for Ruby V3

DisableRegion

Menonaktifkan (opts-out) Wilayah tertentu untuk akun.

> **Note**
>
> Tindakan menonaktifkan suatu Wilayah akan menghapus semua akses IAM ke sumber daya apa pun yang berada di Wilayah tersebut.

Minta Sintaks

```
POST /disableRegion HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Jika Anda tidak menentukan parameter ini, itu default ke identitas Akun AWS yang digunakan untuk memanggil operasi. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di akun manajemen organisasi atau akun administrator yang didelegasikan. ID akun yang ditentukan juga harus menjadi akun anggota di organisasi yang sama. Organisasi harus mengaktifkan semua fitur, dan organisasi harus mengaktifkan akses tepercaya untuk layanan Manajemen Akun, dan secara opsional akun admin yang didelegasikan ditetapkan.

> **Note**
>
> Akun manajemen tidak dapat menentukan sendiri`AccountId`. Ini harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, jangan tentukan parameter ini. Sebagai gantinya, panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau modifikasi.

Jenis: String

Pola: `^\d{12}$`

Diperlukan: Tidak

RegionName

Menentukan Region-kode untuk nama Region tertentu (misalnya,). `af-south-1` Saat Anda menonaktifkan Wilayah, AWS lakukan tindakan untuk menonaktifkan Wilayah tersebut di akun Anda, seperti menghancurkan sumber daya IAM di Wilayah. Proses ini memerlukan waktu beberapa menit untuk sebagian besar akun, tetapi dapat memakan waktu beberapa jam. Anda tidak dapat mengaktifkan Wilayah sampai proses penonaktifan selesai sepenuhnya.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Diperlukan: Ya

Sintaksis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

Kode Status HTTP: 403

ConflictException

Permintaan tidak dapat diproses karena konflik dalam status sumber daya saat ini. Misalnya, ini terjadi jika Anda mencoba mengaktifkan Wilayah yang saat ini sedang dinonaktifkan (dalam status DISABLING).

Kode Status HTTP: 409

InternalServerException

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

Kode Status HTTP: 500

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript

- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

EnableRegion

Mengaktifkan (opts-in) Wilayah tertentu untuk akun.

Minta Sintaks

```
POST /enableRegion HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Jika Anda tidak menentukan parameter ini, itu default ke identitas Akun AWS yang digunakan untuk memanggil operasi. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di akun manajemen organisasi atau akun administrator yang didelegasikan. ID akun yang ditentukan juga harus menjadi akun anggota di organisasi yang sama. Organisasi harus mengaktifkan semua fitur, dan organisasi harus mengaktifkan akses tepercaya untuk layanan Manajemen Akun, dan secara opsional akun admin yang didelegasikan ditetapkan.

> **Note**
>
> Akun manajemen tidak dapat menentukan sendiri`AccountId`. Ini harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, jangan tentukan parameter ini. Sebagai gantinya, panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau modifikasi.

Jenis: String

Pola: `^\d{12}$`

Wajib: Tidak

RegionName

Menentukan Region-kode untuk nama Region tertentu (misalnya,). `af-south-1` Saat mengaktifkan Wilayah, AWS lakukan tindakan untuk mempersiapkan akun Anda di Wilayah tersebut, seperti mendistribusikan sumber daya IAM ke Wilayah. Proses ini memakan waktu beberapa menit untuk sebagian besar akun, tetapi bisa memakan waktu beberapa jam. Anda tidak dapat menggunakan Wilayah sampai proses ini selesai. Selain itu, Anda tidak dapat menonaktifkan Wilayah hingga proses pengaktifan selesai sepenuhnya.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

Kode Status HTTP: 403

ConflictException

Permintaan tidak dapat diproses karena konflik dalam status sumber daya saat ini. Misalnya, ini terjadi jika Anda mencoba mengaktifkan Wilayah yang saat ini sedang dinonaktifkan (dalam status DISABLING).

Kode Status HTTP: 409

InternalServerException

Operasi gagal karena kesalahan internal keAWS. Coba operasi Anda lagi nanti.

Kode Status HTTP: 500

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWSAntarmuka Baris Perintah
- AWSSDK for .NET
- AWSSDK for C++
- AWSSDK for Go
- AWSSDK for Java V2
- AWSSDK untuk V3 JavaScript
- AWSSDK for PHP V3
- AWSSDK untuk Python
- AWSSDK for Ruby V3

GetAlternateContact

Mengambil kontak alternatif yang ditentukan yang dilampirkan ke fileAkun AWS.

Untuk detail selengkapnya tentang cara menggunakan operasi kontak alternatif, lihat Mengakses atau memperbarui kontak alternatif.

> **Note**
>
> Sebelum Anda dapat memperbarui informasi kontak alternatif untuk informasi Akun AWS yang dikelola olehAWS Organizations, Anda harus terlebih dahulu mengaktifkan integrasi antara Manajemen AWS Akun dan Organizations. Untuk informasi selengkapnya, lihat Mengaktifkan akses tepercaya untuk Manajemen AWS Akun.

Minta Sintaks

```
POST /getAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun AWS akun yang ingin Anda akses atau modifikasi dengan operasi ini.

Jika Anda tidak menentukan parameter ini, itu default ke AWS akun identitas yang digunakan untuk memanggil operasi.

Untuk menggunakan parameter ini, pemanggil harus berupa identitas di akun manajemen organisasi atau akun administrator yang didelegasikan, dan ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan semua fitur, dan organisasi harus mengaktifkan akses tepercaya untuk layanan Manajemen Akun, dan secara opsional akun admin yang didelegasikan ditetapkan.

> **Note**
>
> Akun manajemen tidak dapat menentukan sendiri`AccountId`; itu harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, maka jangan tentukan parameter ini, dan panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau ubah.

Jenis: String

Pola: `^\d{12}$`

Wajib: Tidak

AlternateContactType

Menentukan kontak alternatif yang ingin Anda ambil.

Jenis: String

Nilai yang Valid: `BILLING | OPERATIONS | SECURITY`

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "AlternateContact": {
      "AlternateContactType": "string",
      "EmailAddress": "string",
```

```
        "Name": "string",
        "PhoneNumber": "string",
        "Title": "string"
    }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

AlternateContact

Struktur yang berisi rincian untuk kontak alternatif yang ditentukan.

Tipe: Objek AlternateContact

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

Kode Status HTTP: 403

InternalServerException

Operasi gagal karena kesalahan internal keAWS. Coba operasi Anda lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Operasi gagal karena menentukan sumber daya yang tidak dapat ditemukan.

Kode Status HTTP: 404

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

Kode Status HTTP: 400

Contoh

Contoh 1

Contoh berikut mengambil kontak alternatif keamanan untuk akun yang kredensialnya digunakan untuk memanggil operasi.

Sampel Permintaan

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{ "AlternateContactType": "SECURITY" }
```

Contoh Respons

```
HTTP/1.1 200 OK
Content-Type: application/json{
   "AlternateContact": {
        "Name": "Anika",
        "Title": "COO",
        "EmailAddress": "anika@example.com",
        "PhoneNumber": "206-555-0198"
        "AlternateContactType": "Security"
    }
}
```

Contoh 2

Contoh berikut mengambil kontak alternatif operasi untuk akun anggota yang ditentukan dalam suatu organisasi. Anda harus menggunakan kredensi dari akun manajemen organisasi atau dari akun admin yang didelegasikan oleh layanan Manajemen Akun.

Sampel Permintaan

```
POST / HTTP/1.1
```

```
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{ "AccountId": "123456789012", "AlternateContactType": "Operations" }
```

Contoh Respons

```
HTTP/1.1 200 OK
Content-Type: application/json{
   "AlternateContact": {
        "Name": "Anika",
        "Title": "COO",
        "EmailAddress": "anika@example.com",
        "PhoneNumber": "206-555-0198"
        "AlternateContactType": "Operations"
    }
}
```

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWSAntarmuka Baris Perintah
- AWSSDK for .NET
- AWSSDK for C++
- AWSSDK for Go
- AWSSDK for Java V2
- AWSSDK untuk V3 JavaScript
- AWSSDK for PHP V3
- AWSSDK untuk Python
- AWSSDK for Ruby V3

GetContactInformation

Mengambil informasi kontak utama dari file. Akun AWS

Untuk detail selengkapnya tentang cara menggunakan operasi kontak utama, lihat Memperbarui informasi kontak utama dan alternatif.

Minta Sintaks

```
POST /getContactInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Jika Anda tidak menentukan parameter ini, itu default ke identitas Akun AWS yang digunakan untuk memanggil operasi. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di akun manajemen organisasi atau akun administrator yang didelegasikan. ID akun yang ditentukan juga harus menjadi akun anggota di organisasi yang sama. Organisasi harus mengaktifkan semua fitur, dan organisasi harus mengaktifkan akses tepercaya untuk layanan Manajemen Akun, dan secara opsional akun admin yang didelegasikan ditetapkan.

> **Note**
>
> Akun manajemen tidak dapat menentukan sendiri`AccountId`. Ini harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, jangan tentukan parameter ini. Sebagai gantinya, panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau modifikasi.

Jenis: String

Pola: ^\d{12}$

Diperlukan: Tidak

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "ContactInformation": {
      "AddressLine1": "string",
      "AddressLine2": "string",
      "AddressLine3": "string",
      "City": "string",
      "CompanyName": "string",
      "CountryCode": "string",
      "DistrictOrCounty": "string",
      "FullName": "string",
      "PhoneNumber": "string",
      "PostalCode": "string",
      "StateOrRegion": "string",
      "WebsiteUrl": "string"
   }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

ContactInformation

Berisi rincian informasi kontak utama yang terkait dengan fileAkun AWS.

Tipe: Objek ContactInformation

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

Kode Status HTTP: 403

InternalServerException

Operasi gagal karena kesalahan internal keAWS. Coba operasi Anda lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Operasi gagal karena menentukan sumber daya yang tidak dapat ditemukan.

Kode Status HTTP: 404

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWSAntarmuka Baris Perintah
- AWSSDK for .NET

- AWSSDK for C++
- AWSSDK for Go
- AWSSDK for Java V2
- AWSSDK untuk V3 JavaScript
- AWSSDK for PHP V3
- AWSSDK untuk Python
- AWSSDK for Ruby V3

GetRegionOptStatus

Mengambil status keikutsertaan dari Wilayah tertentu.

Minta Sintaks

```
POST /getRegionOptStatus HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Jika Anda tidak menentukan parameter ini, itu default ke identitas Akun AWS yang digunakan untuk memanggil operasi. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di akun manajemen organisasi atau akun administrator yang didelegasikan. ID akun yang ditentukan juga harus menjadi akun anggota di organisasi yang sama. Organisasi harus mengaktifkan semua fitur, dan organisasi harus mengaktifkan akses tepercaya untuk layanan Manajemen Akun, dan secara opsional akun admin yang didelegasikan ditetapkan.

> **Note**
>
> Akun manajemen tidak dapat menentukan sendiri`AccountId`. Ini harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, jangan tentukan parameter ini. Sebagai gantinya, panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau modifikasi.

Jenis: String

Pola: `^\d{12}$`

Wajib: Tidak

RegionName

Menentukan Region-kode untuk nama Region tertentu (misalnya,). `af-south-1` Fungsi ini akan mengembalikan status Wilayah apa pun yang Anda lewatkan ke parameter ini.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "RegionName": "string",
   "RegionOptStatus": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

RegionName

Kode Wilayah yang diteruskan.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

RegionOptStatus

Salah satu status potensial yang dapat dialami Region (Diaktifkan, Mengaktifkan, Dinonaktifkan, Menonaktifkan, Enabled_By_Default).

Jenis: String

Nilai yang Valid: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

Kode Status HTTP: 403

InternalServerException

Operasi gagal karena kesalahan internal keAWS. Coba operasi Anda lagi nanti.

Kode Status HTTP: 500

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWSAntarmuka Baris Perintah
- AWSSDK for .NET
- AWSSDK for C++
- AWSSDK for Go

- AWSSDK for Java V2
- AWSSDK untuk V3 JavaScript
- AWSSDK for PHP V3
- AWSSDK untuk Python
- AWSSDK for Ruby V3

ListRegions

Daftar semua Wilayah untuk akun tertentu dan status keikutsertaannya masing-masing. Secara opsional, daftar ini dapat difilter oleh `region-opt-status-contains` parameter.

Minta Sintaks

```
POST /listRegions HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "MaxResults": number,
   "NextToken": "string",
   "RegionOptStatusContains": [ "string" ]
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Jika Anda tidak menentukan parameter ini, itu default ke identitas Akun AWS yang digunakan untuk memanggil operasi. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di akun manajemen organisasi atau akun administrator yang didelegasikan. ID akun yang ditentukan juga harus menjadi akun anggota di organisasi yang sama. Organisasi harus mengaktifkan semua fitur, dan organisasi harus mengaktifkan akses tepercaya untuk layanan Manajemen Akun, dan secara opsional akun admin yang didelegasikan ditetapkan.

> **Note**
>
> Akun manajemen tidak dapat menentukan sendiri`AccountId`. Ini harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, jangan tentukan parameter ini. Sebagai gantinya, panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau modifikasi.

Jenis: String

Pola: `^\d{12}$`

Wajib: Tidak

MaxResults

Jumlah total item yang akan dikembalikan dalam output perintah. Jika jumlah total item yang tersedia lebih dari nilai yang ditentukan, a `NextToken` disediakan dalam output perintah. Untuk melanjutkan pemberian nomor halaman, berikan nilai `NextToken` dalam argumen `starting-token` dari perintah berikutnya. Jangan gunakan elemen `NextToken` respons langsung di luar AWS CLI. Untuk contoh penggunaan, lihat Pagination di Panduan Pengguna Antarmuka Baris AWS Perintah.

Tipe: Integer

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 50.

Wajib: Tidak

NextToken

Token yang digunakan untuk menentukan di mana harus memulai paginating. Ini adalah `NextToken` dari respons yang sebelumnya terpotong. Untuk contoh penggunaan, lihat Pagination di Panduan Pengguna Antarmuka Baris AWS Perintah.

Jenis: String

Batasan Panjang: Panjang minimum sebesar 0. Panjang maksimum sebesar 1000.

Wajib: Tidak

RegionOptStatusContains

Daftar status Region (Mengaktifkan, Diaktifkan, Menonaktifkan, Dinonaktifkan, Enabled_BY_DEFAULT) untuk digunakan untuk memfilter daftar Wilayah untuk akun tertentu. Misalnya, meneruskan nilai ENABLING hanya akan mengembalikan daftar Wilayah dengan status Region ENABLING.

Tipe: Array string

Nilai yang Valid: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Regions": [
      {
         "RegionName": "string",
         "RegionOptStatus": "string"
      }
   ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

NextToken

Jika ada lebih banyak data yang akan dikembalikan, ini akan diisi. Itu harus diteruskan ke parameter `next-token` permintaan`list-regions`.

Jenis: String

Regions

Ini adalah daftar Wilayah untuk akun tertentu, atau jika parameter yang difilter digunakan, daftar Wilayah yang cocok dengan kriteria filter yang ditetapkan dalam `filter` parameter.

Tipe: Array objek Region

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

Kode Status HTTP: 403

InternalServerException

Operasi gagal karena kesalahan internal keAWS. Coba operasi Anda lagi nanti.

Kode Status HTTP: 500

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWSAntarmuka Baris Perintah
- AWSSDK for .NET
- AWSSDK for C++
- AWSSDK for Go
- AWSSDK for Java V2
- AWSSDK untuk V3 JavaScript
- AWSSDK for PHP V3
- AWSSDK untuk Python

- AWSSDK for Ruby V3

PutAlternateContact

Memodifikasi kontak alternatif yang ditentukan yang dilampirkan ke fileAkun AWS.

Untuk detail selengkapnya tentang cara menggunakan operasi kontak alternatif, lihat Mengakses atau memperbarui kontak alternatif.

> **Note**
>
> Sebelum Anda dapat memperbarui informasi kontak alternatif untuk informasi Akun AWS yang dikelola olehAWS Organizations, Anda harus terlebih dahulu mengaktifkan integrasi antara Manajemen AWS Akun dan Organizations. Untuk informasi selengkapnya, lihat Mengaktifkan akses tepercaya untuk Manajemen AWS Akun.

Minta Sintaks

```
POST /putAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string",
   "EmailAddress": "string",
   "Name": "string",
   "PhoneNumber": "string",
   "Title": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun AWS akun yang ingin Anda akses atau modifikasi dengan operasi ini.

Jika Anda tidak menentukan parameter ini, itu default ke AWS akun identitas yang digunakan untuk memanggil operasi.

Untuk menggunakan parameter ini, pemanggil harus berupa identitas di akun manajemen organisasi atau akun administrator yang didelegasikan, dan ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan semua fitur, dan organisasi harus mengaktifkan akses tepercaya untuk layanan Manajemen Akun, dan secara opsional akun admin yang didelegasikan ditetapkan.

> **Note**
>
> Akun manajemen tidak dapat menentukan sendiri`AccountId`; itu harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, maka jangan tentukan parameter ini, dan panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau ubah.

Jenis: String

Pola: `^\d{12}$`

Wajib: Tidak

AlternateContactType

Menentukan kontak alternatif yang ingin Anda buat atau update.

Jenis: String

Nilai yang Valid: `BILLING | OPERATIONS | SECURITY`

Wajib: Ya

EmailAddress

Menentukan alamat email untuk kontak alternatif.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum adalah 64.

Pola: `^[\s]*[\w+=.#!&-]+@[\w.-]+\.[\w]+[\s]*$`

Diperlukan: Ya

Name

Menentukan nama untuk kontak alternatif.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum adalah 64.

Wajib: Ya

PhoneNumber

Menentukan nomor telepon untuk kontak alternatif.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 25.

Pola: `^[\s0-9()+-]+$`

Diperlukan: Ya

Title

Menentukan judul untuk kontak alternatif.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

Kode Status HTTP: 403

InternalServerException

Operasi gagal karena kesalahan internal keAWS. Coba operasi Anda lagi nanti.

Kode Status HTTP: 500

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

Kode Status HTTP: 400

Contoh

Contoh 1

Contoh berikut menetapkan kontak alternatif penagihan untuk akun yang kredensialnya digunakan untuk memanggil operasi.

Sampel Permintaan

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
    "AlternateContactType": "Billing",
    "Name": "Carlos Salazar",
    "Title": "CFO",
    "EmailAddress": "carlos@example.com",
```

```
    "PhoneNumber": "206-555-0199"
}
```

Contoh Respons

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Contoh 2

Contoh berikut menetapkan atau menimpa kontak alternatif penagihan untuk akun anggota yang ditentukan dalam organisasi. Anda harus menggunakan kredensi dari akun manajemen organisasi atau dari akun admin yang didelegasikan oleh layanan Manajemen Akun.

Sampel Permintaan

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
    "AccountId": "123456789012",
    "AlternateContactType": "Billing",
    "Name": "Carlos Salazar",
    "Title": "CFO",
    "EmailAddress": "carlos@example.com",
    "PhoneNumber": "206-555-0199"
}
```

Contoh Respons

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWSAntarmuka Baris Perintah
- AWSSDK for .NET

- AWSSDK for C++
- AWSSDK for Go
- AWSSDK for Java V2
- AWSSDK untuk V3 JavaScript
- AWSSDK for PHP V3
- AWSSDK untuk Python
- AWSSDK for Ruby V3

PutContactInformation

Memperbarui informasi kontak utama dari fileAkun AWS.

Untuk detail selengkapnya tentang cara menggunakan operasi kontak utama, lihat Memperbarui informasi kontak utama dan alternatif.

Minta Sintaks

```
POST /putContactInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "ContactInformation": {
      "AddressLine1": "string",
      "AddressLine2": "string",
      "AddressLine3": "string",
      "City": "string",
      "CompanyName": "string",
      "CountryCode": "string",
      "DistrictOrCounty": "string",
      "FullName": "string",
      "PhoneNumber": "string",
      "PostalCode": "string",
      "StateOrRegion": "string",
      "WebsiteUrl": "string"
   }
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Jika Anda tidak menentukan parameter ini, itu default ke identitas Akun AWS yang

digunakan untuk memanggil operasi. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di akun manajemen organisasi atau akun administrator yang didelegasikan. ID akun yang ditentukan juga harus menjadi akun anggota di organisasi yang sama. Organisasi harus mengaktifkan semua fitur, dan organisasi harus mengaktifkan akses tepercaya untuk layanan Manajemen Akun, dan secara opsional akun admin yang didelegasikan ditetapkan.

> **Note**
>
> Akun manajemen tidak dapat menentukan sendiri`AccountId`. Ini harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, jangan tentukan parameter ini. Sebagai gantinya, panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau modifikasi.

Jenis: String

Pola: `^\d{12}$`

Wajib: Tidak

ContactInformation

Berisi rincian informasi kontak utama yang terkait dengan fileAkun AWS.

Tipe: Objek ContactInformation

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

Kode Status HTTP: 403

InternalServerException

Operasi gagal karena kesalahan internal keAWS. Coba operasi Anda lagi nanti.

Kode Status HTTP: 500

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWSAntarmuka Baris Perintah
- AWSSDK for .NET
- AWSSDK for C++
- AWSSDK for Go
- AWSSDK for Java V2
- AWSSDK untuk V3 JavaScript
- AWSSDK for PHP V3
- AWSSDK untuk Python
- AWSSDK for Ruby V3

Tindakan terkait lainnyaAWSjasa

Operasi berikut ini terkait denganAWS Account Managementtetapi merupakan bagian dariAWS Organizationsnamespace:

- CreateAccount
- CreateGovCloudAkun
- DescribeAccount

CreateAccount

Parameter`CreateAccount`Operasi API tersedia untuk digunakan hanya dalam konteks organisasi yang dikelola olehAWS Organizationslayanan. Operasi API didefinisikan dalam namespace layanan tersebut.

Untuk informasi selengkapnya, lihatCreateAccountdiAWS OrganizationsReferensi API.

CreateGovCloudAkun

Parameter`CreateGovCloudAccount`Operasi API tersedia untuk digunakan hanya dalam konteks organisasi yang dikelola olehAWS Organizationslayanan. Operasi API didefinisikan dalam namespace layanan tersebut.

Untuk informasi selengkapnya, lihatCreateGovCloudAkundi dalamAWS OrganizationsReferensi API.

DescribeAccount

Parameter`DescribeAccount`Operasi API tersedia untuk digunakan hanya dalam konteks organisasi yang dikelola olehAWS Organizationslayanan. Operasi API didefinisikan dalam namespace layanan tersebut.

Untuk informasi selengkapnya, lihatDescribeAccountdiAWS OrganizationsReferensi API.

Tipe Data

tipe data berikut didukung:

- AlternateContact

- ContactInformation
- Region
- ValidationExceptionField

AlternateContact

Struktur yang berisi rincian kontak alternatif yang terkait dengan akun AWS

Daftar Isi

AlternateContactType

Jenis kontak alternatif.

Jenis: String

Nilai yang Valid: `BILLING | OPERATIONS | SECURITY`

Wajib: Tidak

EmailAddress

Alamat email yang dikaitkan dengan kontak ini.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum adalah 64.

Pola: `^[\s]*[\w+=.#!&-]+@[\w.-]+\.[\w]+[\s]*$`

Wajib: Tidak

Name

Nama yang terkait dengan kontak alternatif ini.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum adalah 64.

Wajib: Tidak

PhoneNumber

Nomor telepon yang terkait dengan kontak alternatif ini.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 25.

Pola: `^[\s0-9()+-]+$`

Wajib: Tidak

Title

Judul yang terkait dengan kontak alternatif ini.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API di salah satu AWS SDK yang khusus bahasa, lihat yang berikut ini:

- AWSSDK for C++
- AWSSDK for Go
- AWSSDK for Java V2
- AWSSDK for Ruby V3

ContactInformation

Berisi rincian informasi kontak utama yang terkait dengan fileAkun AWS.

Daftar Isi

AddressLine1

Baris pertama dari alamat kontak utama.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 60.

Diperlukan: Ya

City

Kota alamat kontak utama.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Diperlukan: Ya

CountryCode

Kode negara dua huruf ISO-3166 untuk alamat kontak utama.

Tipe: String

Kendala Panjang: Panjang tetap 2.

Diperlukan: Ya

FullName

Nama lengkap alamat kontak utama.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Diperlukan: Ya

PhoneNumber

Nomor telepon dari informasi kontak utama. Nomor tersebut akan divalidasi dan, di beberapa negara, diperiksa untuk aktivasi.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 20.

Pola: `^[+][\s0-9()-]+$`

Diperlukan: Ya

PostalCode

Kode pos dari alamat kontak utama.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 20.

Diperlukan: Ya

AddressLine2

Baris kedua dari alamat kontak utama, jika ada.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 60.

Diperlukan: Tidak

AddressLine3

Baris ketiga dari alamat kontak utama, jika ada.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 60.

Diperlukan: Tidak

CompanyName

Nama perusahaan yang terkait dengan informasi kontak utama, jika ada.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Diperlukan: Tidak

DistrictOrCounty

Distrik atau kabupaten dari alamat kontak utama, jika ada.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Diperlukan: Tidak

StateOrRegion

Negara bagian atau wilayah alamat kontak utama. Jika alamat surat berada di Amerika Serikat (AS), nilai dalam bidang ini dapat berupa kode status dua karakter (misalnya,`NJ`) atau nama negara lengkap (misalnya,`New Jersey`). Bidang ini diperlukan di negara-negara berikut:`US`,`CA`,`GB`,`DE`,`JP`,`IN`, dan`BR`.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Diperlukan: Tidak

WebsiteUrl

URL situs web yang terkait dengan informasi kontak utama, jika ada.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Diperlukan: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Go.
- AWSSDK for Java V2
- AWS SDK for Ruby V3

Region

Ini adalah struktur yang menyatakan Wilayah untuk akun tertentu, yang terdiri dari nama dan status keikutsertaan.

Daftar Isi

RegionName

Kode Region dari Region tertentu (misalnya,`us-east-1`).

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Diperlukan: Tidak

RegionOptStatus

Salah satu status potensial yang dapat dialami Region (Diaktifkan, Mengaktifkan, Dinonaktifkan, Menonaktifkan, Enabled_By_Default).

Tipe: String

Nilai yang Valid: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Diperlukan: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Go.
- AWSSDK for Java V2
- AWS SDK for Ruby V3

ValidationExceptionField

Input gagal memenuhi kendala yang ditentukan olehAWS layanan di bidang tertentu.

Daftar Isi

message

Pesan tentang pengecualian validasi.

Tipe: String

Wajib: Ya

name

Nama bidang tempat entri yang tidak valid terdeteksi.

Tipe: String

Wajib: Ya

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API di salah satuAWS SDK khusus bahasa, lihat yang berikut ini:

- AWSSDK for C++
- AWSSDK for Go
- AWSSDK for Java V2
- AWSSDK for Ruby V3

Parameter Umum

Daftar berikut berisi parameter yang digunakan semua tindakan untuk menandatangani permintaan Tanda Tangan Versi 4 dengan string kueri. Setiap parameter khusus tindakan tercantum dalam topik untuk tindakan tersebut. Untuk informasi selengkapnya tentang Signature Versi 4, lihat Menandatangani permintaanAWS API di Panduan Pengguna IAM.

Action

Tindakan yang harus dilakukan.

Tipe: string

Wajib: Ya

Version

Versi API yang ditulis dalam permintaan, dinyatakan dalam format HH-BB-TTTT.

Tipe: string

Wajib: Ya

X-Amz-Algorithm

Algoritme hash yang Anda gunakan untuk membuat tanda tangan permintaan.

Syarat: Tentukan parameter ini ketika Anda menyertakan informasi autentikasi dalam string kueri alih-alih di header otorisasi HTTP.

Tipe: string

Nilai yang Valid: `AWS4-HMAC-SHA256`

Diperlukan: Kondisional

X-Amz-Credential

Nilai lingkup kredensial, yang merupakan string yang menyertakan access key Anda, tanggal, wilayah yang Anda targetkan, layanan yang Anda minta, dan string penghentian ("aws4_request"). Nilai dinyatakan dalam format berikut: access_key/HHBBTTTT/wilayah/layanan/aws4_request.

Untuk informasi selengkapnya, lihat Membuat permintaanAWS API yang ditandatangani di Panduan Pengguna IAM.

Syarat: Tentukan parameter ini ketika Anda menyertakan informasi autentikasi dalam string kueri alih-alih di header otorisasi HTTP.

Tipe: string

Diperlukan: Kondisional

X-Amz-Date

Tanggal yang digunakan untuk membuat tanda tangan. Format harus berupa format dasar ISO 8601 (YYYYMMDD'T'HMMSS'Z'). Misalnya, waktu tanggal berikut adalah nilai X-Amz-Date yang valid: `20120325T120000Z`.

Syarat: X-Amz-Date bersifat opsional untuk semua permintaan; nilai ini dapat digunakan untuk mengganti tanggal yang digunakan untuk menandatangani permintaan. Jika header Tanggal ditentukan dalam format dasar ISO 8601, X-Amz-Date tidak diperlukan. Ketika X-Amz-Date digunakan, ia selalu mengganti nilai header Tanggal. Untuk informasi selengkapnya, lihat Elemen tanda tangan permintaanAWS API di Panduan Pengguna IAM.

Tipe: string

Diperlukan: Kondisional

X-Amz-Security-Token

Token keamanan sementara yang diperoleh melalui panggilan keAWS Security Token Service (AWS STS). Untuk daftar layanan yang mendukung kredenial keamanan sementara dariAWS STS, lihat Layanan AWSbahwa bekerja dengan IAM dalam Panduan Pengguna IAM.

Syarat: Jika Anda menggunakan kredenial keamanan sementara dariAWS STS, Anda harus menyertakan token keamanan.

Tipe: string

Diperlukan: Kondisional

X-Amz-Signature

Menentukan tanda tangan yang dikodekan oleh hex yang dihitung dari string to sign dan kunci penandatanganan turunan.

Syarat: Tentukan parameter ini ketika Anda menyertakan informasi autentikasi dalam string kueri alih-alih di header otorisasi HTTP.

Tipe: string

Diperlukan: Kondisional

X-Amz-SignedHeaders

Menentukan semua header HTTP yang disertakan sebagai bagian dari permintaan kanonik. Untuk informasi selengkapnya tentang menentukan header yang ditandatangani, lihat Membuat permintaanAWS API yang ditandatangani di Panduan Pengguna IAM.

Syarat: Tentukan parameter ini ketika Anda menyertakan informasi autentikasi dalam string kueri alih-alih di header otorisasi HTTP.

Tipe: string

Diperlukan: Kondisional

Kesalahan Umum

Bagian ini berisi daftar kesalahan yang umum terjadi pada tindakan API dari semua layanan AWS. Untuk kesalahan khusus pada tindakan API untuk layanan ini, lihat topik untuk tindakan API tersebut.

AccessDeniedException

Anda tidak memiliki akses yang memadai untuk melakukan tindakan ini.

Kode Status HTTP: 400

IncompleteSignature

Tanda tangan permintaan tidak sesuai dengan standar AWS.

Kode Status HTTP: 400

InternalFailure

Pemrosesan permintaan telah gagal karena kesalahan yang tidak diketahui, pengecualian atau kegagalan.

Kode Status HTTP: 500

InvalidAction

Tindakan atau operasi yang diminta tidak valid. Verifikasi bahwa tindakan diketik dengan benar.

Kode Status HTTP: 400

InvalidClientTokenId

Sertifikat X.509 atau access key ID AWS yang diberikan tidak ada dalam catatan kami.

Kode Status HTTP: 403

NotAuthorized

Anda tidak memiliki izin untuk melakukan tindakan ini.

Kode Status HTTP: 400

OptInRequired

Access key ID AWS membutuhkan berlangganan untuk layanan.

Kode Status HTTP: 403

RequestExpired

Permintaan menjangkau layanan lebih dari 15 menit setelah stempel tanggal pada permintaan atau lebih dari 15 menit setelah tanggal kedaluwarsa permintaan (seperti untuk URL pre-signed), atau stempel tanggal pada permintaan lebih dari 15 menit di masa mendatang.

Kode Status HTTP: 400

ServiceUnavailable

Permintaan telah gagal karena kegagalan sementara server.

Kode Status HTTP: 503

ThrottlingException

Permintaan ditolak karena throttling permintaan.

Kode Status HTTP: 400

ValidationError

Input gagal untuk memenuhi batasan yang ditentukan oleh layanan AWS.

Kode Status HTTP: 400

Memanggil API dengan membuat permintaan Kueri HTTP

Bagian ini berisi informasi umum tentang penggunaan Query API untukAWSManajemen Akun. Untuk detail tentang operasi dan kesalahan API, lihatReferensi API.

> **Note**
>
> Alih-alih melakukan panggilan langsung keAWSAccount Management Query API, Anda dapat menggunakan salah satuAWSSDK. SDK AWS terdiri atas perpustakaan dan kode sampel untuk berbagai bahasa dan platform pemrograman (Java, Ruby, .NET, iOS, Android, dan banyak lagi). SDK menyediakan cara mudah untuk membuat akses terprogram keAWSManajemen Akun danAWS. Misalnya, SDK menangani tugas seperti menandatangani permintaan secara kriptografis, mengelola kesalahan, dan mencoba kembali permintaan secara otomatis. Untuk informasi tentang AWS SDK, termasuk cara mengunduh dan menginstalnya, lihat Alat untuk Amazon Web Services.

Dengan Query API untukAWSManajemen Akun, Anda dapat memanggil tindakan layanan. Permintaan API kueri adalah permintaan HTTPS yang harus berisi`Action`parameter untuk menunjukkan operasi yang akan dilakukan.AWS Dukungan Manajemen Akun`GET`dan`POST`permintaan untuk semua operasi. Artinya, API tidak mengharuskan Anda untuk menggunakan`GET`untuk beberapa tindakan dan`POST`untuk orang lain. Namun,`GET`permintaan tunduk pada ukuran batasan URL. Meskipun batas ini bergantung pada browser, batas tipikal adalah 2.048 byte. Oleh karena itu, untuk permintaan Query API yang membutuhkan ukuran yang lebih besar, Anda harus menggunakan`POST`permintaan.

Responsnya adalah dokumen XML. Untuk detail tentang respons, lihat halaman tindakan individual diReferensi API.

Topik

- Titik akhir
- HTTPS diperlukan
- PenandatangananAWSPermintaan API Manajemen Akun

Titik akhir

AWSManajemen Akun memiliki titik akhir API global tunggal yang dihosting di AS Timur (Virginia Utara)Wilayah AWS.

Untuk informasi lebih lanjut tentangAWSendpoint dan Wilayah untuk semua layanan, lihatWilayah dan Titik Akhirdi dalamReferensi Umum AWS.

HTTPS diperlukan

Karena Query API dapat mengembalikan informasi sensitif seperti kredensi keamanan, Anda harus menggunakan HTTPS untuk mengenkripsi semua permintaan API.

PenandatangananAWSPermintaan API Manajemen Akun

Permintaan harus ditandatangani menggunakan access key ID dan secret access key. Kami sangat menyarankan agar Anda tidak menggunakanAWSkredensi akun root untuk pekerjaan sehari-hari denganAWSManajemen Akun. Anda dapat menggunakan kredensi untukAWS Identity and Access Management(IAM) pengguna atau kredensi sementara seperti yang Anda gunakan dengan peran IAM.

Untuk menandatangani permintaan API Anda, Anda harus menggunakan Tanda Tangan Versi 4 AWS. Untuk informasi tentang penggunaan Signature Versi 4, lihatPenandatangananAWSPermintaan APIdi dalamPanduan Pengguna IAM.

Untuk informasi selengkapnya, lihat yang berikut:

- AWSKredensial Keamanan— Menyediakan informasi umum tentang jenis kredensi yang dapat Anda gunakan untuk mengaksesAWS.
- Praktik terbaik keamanan di IAM— Menawarkan saran untuk menggunakan layanan IAM untuk membantu mengamankan AndaAWSsumber daya, termasuk yang ada diAWSManajemen Akun.
- Kredensi keamanan sementara di IAM- Menjelaskan cara membuat dan menggunakan kredensi keamanan sementara.

Kuota untuk AWS Account Management

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk setiap layanan. AWS Kecuali dinyatakan lain, setiap kuota adalah Wilayah AWS -spesifik.

Masing-masing Akun AWS memiliki kuota berikut yang terkait dengan Manajemen Akun.

Resource	Kuota
Jumlah kontak alternatif dalam Akun AWS	3 - masing-masing untuk`BILLING`,`SECURITY`, dan `OPERATIONS`
Jumlah permintaan pilihan wilayah bersamaan per akun	6
Jumlah permintaan pilihan wilayah bersamaan per organisasi	20
Tarif `DeleteAlternateContact` permintaan per akun	1 per detik, meledak menjadi 6 per detik
Tarif `DisableRegion` permintaan per akun	1 per detik, meledak menjadi 1 per detik
Tarif `EnableRegion` permintaan per akun	1 per detik, meledak menjadi 1 per detik
Tarif `GetAlternateContact` permintaan per akun	10 per detik, meledak menjadi 15 per detik
Tarif `GetContactInformation` permintaan per akun	10 per detik, meledak menjadi 15 per detik
Tarif `GetRegionOptStatus` permintaan per akun	5 per detik, meledak menjadi 5 per detik
Tarif `ListRegions` permintaan per akun	5 per detik, meledak menjadi 5 per detik
Tarif `PutAlternateContact` permintaan per akun	5 per detik, meledak menjadi 8 per detik

Resource	Kuota
Tarif `PutContactInformation` permintaan per akun	5 per detik, meledak menjadi 8 per detik

Memecahkan masalah Anda Akun AWS

Gunakan informasi dalam topik berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah AndaAkun AWS. Untuk bantuan dengan pengguna root, lihat Memecahkan masalah dengan pengguna root di Panduan Pengguna IAM. Untuk bantuan terkait proses login, lihat Memecahkan masalah Akun AWS login di Panduan Pengguna Masuk. AWS

Topik-topik penyelesaian masalah

- Memecahkan masalah dengan pembuatan Akun AWS
- Memecahkan masalah dengan penutupan Akun AWS
- Pemecahan masalah lainnya denganAkun AWS

Memecahkan masalah dengan pembuatan Akun AWS

Gunakan informasi di sini untuk membantu Anda memecahkan masalah yang terkait dengan pembuatan file. Akun AWS Jika Anda mengalami masalah saat masuk ke akun baru setelah dibuat, lihat Memecahkan masalah Akun AWS login di Panduan Masuk. AWS

Masalah

- Saya tidak menerima panggilan dari AWS untuk memverifikasi akun baru saya
- Saya mendapatkan kesalahan tentang “jumlah maksimum upaya yang gagal” ketika saya mencoba memverifikasi Akun AWS melalui telepon
- Sudah lebih dari 24 jam dan akun saya tidak diaktifkan

Saya tidak menerima panggilan dari AWS untuk memverifikasi akun baru saya

Saat Anda membuatAkun AWS, Anda harus memberikan nomor telepon tempat Anda dapat menerima pesan SMS atau panggilan suara. Anda menentukan metode mana yang akan digunakan untuk memverifikasi nomor.

Jika Anda tidak menerima pesan atau panggilan, verifikasi hal berikut:

- Anda memasukkan nomor telepon yang benar dan memilih kode negara yang benar selama proses pendaftaran.

- Jika Anda menggunakan ponsel, pastikan Anda memiliki sinyal seluler untuk menerima pesan atau panggilan SMS.
- Informasi yang Anda masukkan untuk metode pembayaran Anda benar.

Jika Anda tidak menerima SMS atau panggilan untuk menyelesaikan proses verifikasi identitas, AWS Support dapat membantu Anda untuk mengaktifkan Akun AWS secara manual. Gunakan langkah-langkah berikut:

1. Pastikan Anda dapat dihubungi di nomor telepon yang Anda berikan untuk AndaAkun AWS.
2. Buka AWS Supportkonsol, lalu pilih Buat kasus.
   a. Pilih Support akun dan penagihan.
   b. Untuk Jenis, pilih Akun.
   c. Untuk Kategori, pilih Aktivasi.
   d. Di bagian Deskripsi kasus, berikan tanggal dan waktu kapan Anda dapat dihubungi.
   e. Di bagian Opsi kontak, pilih Metode Obrolan untuk Kontak.
   f. Pilih Submit (Kirim).

> **Note**
>
> Anda dapat membuat kasus dengan AWS Support bahkan jika Anda Akun AWS belum diaktifkan.

Saya mendapatkan kesalahan tentang “jumlah maksimum upaya yang gagal” ketika saya mencoba memverifikasi Akun AWS melalui telepon

AWS Supportdapat membantu Anda mengaktifkan akun Anda secara manual. Ikuti langkah-langkah ini:

1. Masuk ke Anda Akun AWS menggunakan alamat email dan kata sandi yang Anda tentukan saat membuat akun.
2. Buka AWS Supportkonsol, lalu pilih Buat kasus.
3. Pilih Akun dan Dukungan Penagihan.
4. Untuk Jenis, pilih Akun.

5. Untuk Kategori, pilih Aktivasi.
6. Di bagian Deskripsi kasus, berikan tanggal dan waktu kapan Anda dapat dihubungi.
7. Di bagian Opsi kontak, pilih Metode Obrolan untuk Kontak.
8. Pilih Submit (Kirim).

AWS Supportakan menghubungi Anda dan mencoba untuk mengaktifkan Anda secara manualAkun AWS.

Sudah lebih dari 24 jam dan akun saya tidak diaktifkan

Aktivasi akun terkadang dapat ditunda. Jika prosesnya memakan waktu lebih dari 24 jam, periksa hal berikut:

- Selesaikan proses aktivasi akun.

  Jika Anda menutup jendela untuk proses pendaftaran sebelum Anda menambahkan semua informasi yang diperlukan, buka halaman pendaftaran. Pilih Masuk ke yang sudah ada Akun AWS, dan masuk menggunakan alamat email dan kata sandi yang Anda pilih untuk akun tersebut.
- Periksa informasi yang terkait dengan metode pembayaran Anda.

  Di AWS Billing and Cost Management konsol, periksa Metode Pembayaran untuk kesalahan.
- Hubungi lembaga keuangan Anda.

  Terkadang lembaga keuangan menolak permintaan otorisasi dari. AWS Hubungi lembaga yang terkait dengan metode pembayaran Anda, dan minta mereka untuk menyetujui permintaan otorisasi dari. AWS AWSmembatalkan permintaan otorisasi segera setelah disetujui oleh lembaga keuangan Anda, sehingga Anda tidak dikenakan biaya untuk permintaan otorisasi. Permintaan otorisasi mungkin masih muncul sebagai biaya kecil (biasanya 1 USD) pada laporan dari lembaga keuangan Anda.
- Periksa folder email dan spam Anda untuk permintaan informasi tambahan.
- Coba browser yang berbeda.
- KontakAWS Support.

  Hubungi AWS Supportuntuk bantuan. Sebutkan langkah-langkah pemecahan masalah yang sudah Anda coba.

> **Note**
>
> Jangan memberikan informasi sensitif, seperti nomor kartu kredit, dalam korespondensi apa pun denganAWS.

Memecahkan masalah dengan penutupan Akun AWS

Gunakan informasi di bawah ini untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang ditemukan selama proses penutupan akun. Untuk informasi umum tentang proses penutupan akun, lihatTutup sebuah Akun AWS.

Topik

- Saya tidak tahu cara menghapus atau membatalkan akun saya
- Saya tidak melihat tombol Tutup akun di halaman Akun
- Saya menutup akun saya tetapi masih belum menerima konfirmasi email
- Saya menerima kesalahan ConstraintViolationException "" saat mencoba menutup akun saya
- Saya menerima kesalahan “CLOSE_ACCOUNT_QUOTA_EXCEEDED” saat mencoba menutup akun anggota
- Apakah saya perlu menghapus AWS organisasi saya sebelum menutup akun manajemen?

Saya tidak tahu cara menghapus atau membatalkan akun saya

Untuk menutup akun Anda, ikuti instruksi diTutup sebuah Akun AWS.

Saya tidak melihat tombol Tutup akun di halaman Akun

Jika Anda tidak masuk sebagai pengguna root, Anda tidak akan melihat tombol Tutup akun yang ditampilkan di halaman Akun. Anda harus Masuk ke AWS Management Console sebagai pengguna root untuk menutup akun Anda. Jika Anda tidak dapat masuk, lihat Memecahkan masalah dengan pengguna root.

Saya menutup akun saya tetapi masih belum menerima konfirmasi email

Email konfirmasi ini hanya dikirim ke alamat email pengguna root untuk file Akun AWS. Jika Anda tidak menerima email ini dalam beberapa jam, Anda dapat Masuk ke AWS Management Console

sebagai pengguna root untuk memeriksa apakah akun Anda ditutup. Jika akun Anda berhasil ditutup, Anda akan melihat pesan yang ditampilkan yang menunjukkan akun Anda ditutup. Jika akun yang Anda tutup adalah akun anggota, Anda dapat memverifikasi penutupan yang berhasil dengan memeriksa apakah akun yang ditutup diberi label seperti SUSPENDED di AWS Organizations konsol. Untuk informasi selengkapnya, lihat Menutup akun anggota di organisasi Anda di PanduanAWS Organizations Pengguna.

Jika Anda mencoba menutup akun manajemen dan tidak menerima konfirmasi email tentang penutupan akun, organisasi Anda kemungkinan besar memiliki akun anggota aktif. Anda hanya dapat menutup akun manajemen jika organisasi Anda tidak memiliki akun anggota aktif. Untuk memverifikasi bahwa tidak ada akun anggota aktif yang tersisa di organisasi Anda, buka AWS Organizations konsol, dan pastikan semua akun anggota ditampilkan di Suspended sebelah nama akun mereka. Setelah itu, Anda dapat menutup akun manajemen.

Saya menerima kesalahan ConstraintViolationException "" saat mencoba menutup akun saya

Anda mencoba menutup akun manajemen menggunakan AWS Organizations konsol, yang tidak mungkin. Untuk menutup akun manajemen, Anda harus Masuk ke AWS Management Console sebagai pengguna root untuk akun manajemen dan menutupnya dari halaman Akun. Untuk informasi selengkapnya, lihat Menutup akun manajemen di organisasi Anda di PanduanAWS Organizations Pengguna.

Saya menerima kesalahan “CLOSE_ACCOUNT_QUOTA_EXCEEDED” saat mencoba menutup akun anggota

Anda hanya dapat menutup 10% akun anggota dalam periode 30 hari bergulir. Kuota ini tidak terikat oleh bulan kalender, tetapi dimulai ketika Anda menutup akun. Dalam 30 hari sejak penutupan akun awal, Anda tidak dapat melebihi batas penutupan akun 10%. Penutupan akun minimum adalah 10 dan penutupan akun maksimum adalah 1000, bahkan jika 10% akun melebihi 1000. Untuk informasi selengkapnya tentang kuota Organizations, lihat Kuota untuk AWS Organizations di AWS Organizations Panduan Pengguna.

Apakah saya perlu menghapus AWS organisasi saya sebelum menutup akun manajemen?

Tidak, Anda tidak perlu menghapus AWS organisasi Anda sebelum menutup akun manajemen. Namun, Anda hanya dapat menutup akun manajemen jika organisasi Anda tidak memiliki akun

anggota aktif. Untuk memverifikasi bahwa tidak ada akun anggota aktif yang tersisa di organisasi Anda, buka AWS Organizations konsol, dan pastikan semua akun anggota ditampilkan di `Suspended` sebelah nama akun mereka. Setelah itu, Anda dapat menutup akun manajemen.

Pemecahan masalah lainnya denganAkun AWS

Gunakan informasi di sini untuk membantu Anda memecahkan masalah yang terkait denganAkun AWS.

Masalah

- Saya perlu mengubah kartu kredit untuk sayaAkun AWS
- Saya ingin melaporkan penipuanAkun AWSaktivitas
- Saya ingin menutupAkun AWS

Saya perlu mengubah kartu kredit untuk sayaAkun AWS

Untuk mengubah kartu kredit untuk AndaAkun AWS, Anda harus dapat masuk.AWSmemiliki perlindungan yang mengharuskan Anda membuktikan bahwa Anda adalah pemilik akun. Untuk instruksi, lihatMengelola metode pembayaran kartu kredit AndadiAWS BillingPanduan Pengguna.

Saya ingin melaporkan penipuanAkun AWSaktivitas

Jika Anda mencurigai aktivitas penipuan menggunakanAkun AWSdan ingin membuat laporan, lihatBagaimana cara melaporkan penyalahgunaanAWSsumber daya.

Jika Anda mengalami masalah dengan pembelian yang dilakukan di Amazon.com, lihatLayanan Pelanggan Amazon.

Saya ingin menutupAkun AWS

Untuk bantuan memecahkan masalah dengan menutup masalahAkun AWS, lihatTutup sebuah Akun AWS.

Riwayat dokumen untuk Panduan Pengguna Manajemen Akun

Tabel berikut menjelaskan rilis dokumentasi untuk Manajemen AWS Akun.

Perubahan	Deskripsi	Tanggal
Menulis ulang topik akun tutup	Sepenuhnya merombak seluruh topik akun penutupan termasuk menambahkan langkah-langkah untuk cara menutup akun anggota dan manajemen.	Februari 1, 2024
Akhir dukungan untuk menambahkan pertanyaan tantangan keamanan baru	Menambahkan konten baru yang mencatat bahwa opsi untuk menambahkan pertanyaan tantangan baru telah dihapus dari halaman Akun.	Januari 5, 2024
Akhir dukungan untuk `aws-portal` namespace	AWS Identity and Access Management(IAM) tindakan yang sebelumnya digunakan untuk mengelola akun Anda (misalnya, `aws-portal:ModifyAccount` dan`aws-portal:ViewAccount`) telah mencapai akhir dukungan standar.	Januari 1, 2024
Menulis ulang topik Daerah	Merombak seluruh topik Wilayah sepenuhnya termasuk menambahkan kontrol perluas dan ciutkan.	Oktober 8, 2023

Memindahkan topik pengguna root ke Panduan Pengguna IAM	Diskusi konsolidasi tentang pengguna root ke dalam satu topik, menambahkan tautan referensi silang ke topik pengguna root yang dipindahkan ke Panduan Pengguna IAM.	18 September 2023
Bagian baru ditambahkan ke topik kontak akun utama	Menambahkan nomor Telepon baru dan bagian persyaratan alamat email.	12 September 2023
API informasi kontak baru	Support untuk yang baru `GetContactInformation` dan `PutContactInformation` API.	22 Juli 2022
AWSManajemen Akun sekarang mendukung pembaruan kontak alternatif melalui AWS Organizations konsol.	Sekarang Anda dapat memperbarui kontak alternatif organisasi Anda melalui AWS Organizations konsol menggunakan izin API Akun yang disediakan oleh kebijakan AWS Organizations terkelola yang diperbarui.	8 Februari 2022
Rilis awal	Rilis awal Panduan Referensi Manajemen AWS Akun	30 September 2021

AWSGlosarium

Untuk AWS terminologi terbaru, lihat AWSglosarium di Referensi. Glosarium AWS

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.